

# Yet More Elements in the Shafarevich-Tate Group of the Jacobian of a Fermat Curve

Benjamin Levitt and William McCallum

ABSTRACT. For certain irregular primes  $p$  we construct non-trivial elements in the Shafarevich-Tate group of the jacobian of a quotient of the Fermat curve  $x^p + y^p = 1$ . These elements are different in general from elements previously constructed by McCallum and McCallum-Tzermias.

## 1. Introduction

For an odd prime number  $p$  and an integer  $s$  with  $1 \leq s \leq p - 2$ , the complete nonsingular curve  $F_s$  with equation

$$y^p = x^s(1 - x)$$

is a quotient of the Fermat curve  $x^p + y^p = 1$ . It has genus  $(p - 1)/2$  and its jacobian  $J$  has complex multiplication by  $\mathbb{Z}[\mu_p]$ , where  $\mu_p$  is the group of  $p$ -th roots of unity in  $\overline{\mathbb{Q}}$ . In this paper we construct non-trivial elements in the  $p$ -torsion of the Shafarevich-Tate group

$$\text{III} = \text{III}(J, \mathbb{Q}(\mu_p))$$

for certain irregular primes  $p$ . These are new elements, in the sense that there is not in general any linear dependence relation over  $\mathbb{Z}[\mu_p]$  between them and ones previously constructed [McC88], [MT03]. This result is of interest because a Selmer group calculation shows that, if  $\mathfrak{p}$  is the prime ideal in  $\mathbb{Z}[\mu_p]$  above  $p$ , then

$$\text{rank}_{\mathbb{Z}/p\mathbb{Z}} \text{III}/\mathfrak{p} + \text{rank}_{\mathbb{Z}/p\mathbb{Z}} J(\mathbb{Q}(\mu_p))/\mathfrak{p}$$

is relatively large: heuristically, it is asymptotic to  $p/4$  as  $p$  grows [McC92, Theorem 1 and introductory discussion]. Thus we should be able to find either an abundance of  $\mathbb{Z}[\mu_p]$ -independent elements in  $\text{III}$  or an abundance of  $\mathbb{Z}[\mu_p]$ -independent points in  $J(\mathbb{Q}(\mu_p))$ . The current result adds to the growing body of circumstantial evidence that it is easier to do the former. Indeed, modulo torsion, the only systematically occurring explicitly known infinite  $\mathbb{Z}[\mu_p]$ -submodule of  $J(\mathbb{Q}(\mu_p))$  is the one generated by the Gross-Rohrlich point [GR78].

Consider the usual descent sequence

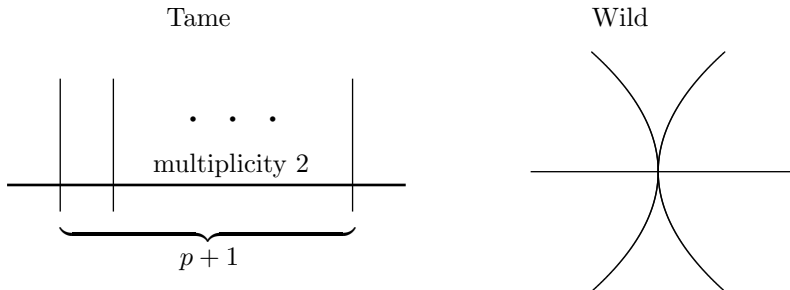
$$0 \rightarrow J(\mathbb{Q}(\mu_p))/\lambda^k J(\mathbb{Q}(\mu_p)) \rightarrow S_{\lambda^k} \rightarrow \text{III}[\lambda^k] \rightarrow 0,$$

---

2000 *Mathematics Subject Classification*. Primary 11G30; Secondary 14G25, 14K15.

*Key words and phrases*. Shafarevich-Tate group, Fermat curve, Jacobian.

The authors were supported in part by NSF grant DUE 0525009.

FIGURE 1. Reduction types of  $F_s$ 

where  $\lambda$  is a generator of  $\mathfrak{p}$  and  $S_{\lambda^k} = S_{\lambda^k}(J, \mathbb{Q}(\mu_p))$  is the Selmer group associated with a positive integer power  $\lambda^k$ . A choice of group isomorphism between  $J[\lambda]$  and the group  $\mu_p$  of  $p$ -th roots of unity enables us to identify  $S_{\lambda}(J, \mathbb{Q}(\mu_p))$  with a subgroup of  $\mathbb{Q}(\mu_p)^\times / \mathbb{Q}(\mu_p)^{\times p}$ . The two previous non-triviality results and the one we prove in this paper depend on finding a specific element  $\eta \in \mathbb{Q}(\mu_p)^\times / \mathbb{Q}(\mu_p)^{\times p}$  which is contained in  $S_{\lambda}$  under this identification and, for some  $k$ , lifts to an element of  $S_{\lambda^k}$  whose image in  $\text{III}$  is non-trivial.

The elements  $\eta$  come from cyclotomic units, as follows. Let  $\Delta = \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ , let  $\omega : \Delta \rightarrow \mathbb{Z}_p^\times$  be the Teichmüller character, and define for any integer  $i$  the usual idempotent

$$\epsilon_i = \frac{1}{p-1} \sum_{\sigma \in \Delta} \omega^{-i}(\sigma) \sigma.$$

Fix a primitive  $p$ -th root of unity  $\zeta$ , and define  $\eta_i \in \mathbb{Q}(\mu_p)^\times / \mathbb{Q}(\mu_p)^{\times p}$  by<sup>1</sup>

$$(1.1) \quad \eta_i = (1 - \zeta)^{\epsilon_i}.$$

If  $i$  is even,  $2 \leq i \leq p-3$ , and  $p$  does not divide the Bernoulli number  $B_i$ , then  $\eta_i$  is locally non-trivial at  $p$  (that is, its image in  $\mathbb{Q}_p(\mu_p)^\times / \mathbb{Q}_p(\mu_p)^{\times p}$  is nonzero) [Was97, Chapter 8]. Furthermore, by eigenvalue considerations the nontrivial elements among the  $\eta_i$  with  $2 \leq i \leq p-1$  are linearly independent.

We first recall the nontriviality results of McCallum and McCallum-Tzermias. These depend on computing the Cassels pairing of certain elements. The Cassels pairing

$$\text{III} \times \text{III} \rightarrow \mathbb{Q}/\mathbb{Z}.$$

is skew-symmetric and its kernel is the infinitely divisible subgroup of  $\text{III}$  (a subgroup which is conjectured to be trivial). Its definition is reviewed in [McC88]. The computation depends on local  $p$ -adic analytic approximations of functions on  $F_s$ , and these approximations depend on a minimal regular model for  $F_s$  over  $\mathbb{Z}_p[\mu_p]$ . The special fiber for such a model is a curve over the finite field  $\mathbb{F}_p$  with  $p$  elements, and has two possible geometric types, wild and tame, shown in Figure 1. The terminology corresponds to the ramification type of a field of good reduction for  $F_s$ . The wild type is further divided into split and non-split, according to whether the two

<sup>1</sup>Note that the notation is different from that used in [MS03]. The element  $\eta_i$  defined there is equal to the element  $\eta_{p-i}$  defined here.

tangent components are defined over  $\mathbb{F}_p$  or conjugate over a quadratic extension. The reduction type can be computed as follows. For a rational number  $x$  relatively prime to  $p$  let  $q(x) = (x^{p-1} - 1)/p$ , and let  $\epsilon$  be the Legendre symbol

$$\epsilon = \left( \frac{2s(s+1)q(s^s/(s+1)^{s+1})}{p} \right).$$

Then the reduction type of  $F_s$  is

tame	if $\epsilon = 0$
wild split	if $\epsilon = 1$
wild non-split	if $\epsilon = -1$ .

The first nontriviality theorem that we want to recall here is

**THEOREM 1.1** (McCallum [MT03]). *Suppose  $p$  and  $F_s$  satisfy the following conditions:*

- (1)  $p \equiv 1 \pmod{4}$
- (2)  $p \nmid B_{(p-1)/2} B_{(p+3)/2}$
- (3)  $F_s$  has wild split reduction at  $\mathfrak{p}$ .

*Then the image in  $\text{III}$  of the subgroup of  $S_\lambda$  generated by  $\eta_{(p-1)/2}$  and  $\eta_{(p+3)/2}$  is isomorphic to  $(\mathbb{Z}/p\mathbb{Z})^2$ .*

An example of a curve satisfying the conditions of Theorem 1.1 is  $y^{17} = x(1-x)$ . The proof of the theorem is a calculation of the Cassels pairing between the images of  $\eta_{(p-1)/2}$  and  $\eta_{(p+3)/2}$  in  $\text{III}[\lambda]$ .

The next theorem rests on an extension of the methods in the previous theorem to a calculation of the Cassels pairing between  $\text{III}[\lambda]$  and  $\text{III}[\lambda^3]$ .

**THEOREM 1.2** (McCallum-Tzermias [MT03]). *Suppose that  $p$  and  $s$  satisfy the following conditions:*

- (1)  $p \geq 19$  is regular and  $p \equiv 3 \pmod{4}$
- (2)  $F_s$  has tame or wild non-split reduction at  $\mathfrak{p}$
- (3)  $s$  satisfies the congruence

$$q(s^s/(s+1)^{s+1})^3 - s(s+1)B_{p-3} \not\equiv 0 \pmod{p},$$

where  $q(x) = (x^{p-1} - 1)/p$ .

*Then  $\eta_{(p+5)/2}$  lifts to an element of  $S_{\lambda^3}$ , and this element and the element  $\eta_{(p+1)/2} \in S_\lambda$  have  $\mathbb{Z}$ -independent nontrivial images in  $\text{III}$ .*

An example of a curve satisfying the conditions of Theorem 1.2 is

$$y^{19} = x^2(1-x).$$

In this paper we prove a new non-triviality result. Since  $J$  has good reduction outside  $p$  and  $\deg \lambda = p$ ,  $S_{\lambda^k}$  is contained in  $H^1(G, J[\lambda^k])$ , where  $G$  is the Galois group of the maximal extension of  $\mathbb{Q}(\mu_p)$  unramified outside  $p$ . Our result makes use of the cup product pairing

$$H^1(G, \mu_p) \times H^1(G, \mu_p) \rightarrow H^2(G, \mu_p) \otimes \mu_p,$$

which gives rise to a pairing

$$(1.2) \quad \langle \cdot, \cdot \rangle : E/E^p \times E/E^p \rightarrow H^2(G, \mu_p) \otimes \mu_p = C/pC \otimes \mu_p,$$

where  $E$  is the group of  $p$ -units and  $C$  is the ideal class group of  $\mathbb{Z}[\mu_p]$ . This pairing was studied in [MS03] and shown to be nontrivial for  $p = 37$ . Sharifi subsequently showed the non-triviality of the pairing for  $p \leq 1,000$  [Sha07].

**THEOREM 1.3.** *Suppose that  $p$ ,  $s$ , and  $r$  satisfy the following conditions*

- (1)  $r$  is even and  $2 \leq r \leq (p+1)/2$
- (2)  $F_s$  has wild non-split or tame reduction at  $\mathfrak{p}$
- (3)  $\langle \eta_{p-r+3}, \eta_{p-3} \rangle \neq 0$  (which implies  $p|B_r$ ).

*Then  $\eta_{p-r+3}$  lifts to an element of  $S_{\lambda^3}$  whose image in III is nontrivial.*

Note that condition (3) implies that  $p$  must be an irregular prime for Theorem 1.3 to apply. An example of a curve satisfying the conditions of Theorem 1.3 is  $y^{691} = x(1-x)$ . It has wild non-split reduction, and 691 divides both  $B_{12}$  and  $B_{200}$ . Both  $r = 12$  and  $r = 200$  satisfy condition (2), and  $\langle \eta_{682}, \eta_{688} \rangle$  and  $\langle \eta_{494}, \eta_{688} \rangle$  are both non-zero [MS03, Sha07]. This gives us two independent elements of order 691 in III.

We would like to thank the referee for several useful comments and corrections.

## 2. Galois structure of the $\lambda^4$ -torsion

The divisor  $(0,0) - \infty$  on  $F_s$  is fixed by  $\zeta$  and therefore represents a nontrivial  $\mathbb{Q}$ -rational  $\lambda$ -torsion point. Let  $K = \mathbb{Q}(\mu_p)$ . Greenberg determined the field of definition of the higher  $\lambda$ -torsion:

**THEOREM 2.1** (Greenberg [Gre81]). *We have*

$$K(J[\lambda^3]) = K$$

and

$$K(J[\lambda^4]) = K(\eta_{p-3}^{1/p}).$$

The first part is Theorem 1 of the cited reference. Although the second part is not explicitly stated, the proof is contained in the first paragraph of Section 5. (The condition  $\omega^i(a+1) = \omega^i(a)+1$  stated in the reference boils down to  $(s+1)^3 \equiv s^3+1 \pmod{p}$ , which is trivially satisfied.)

Theorem 2.1 enables us to determine explicitly the structure of  $J[\lambda^4]$  as a Galois module over  $K$ . Following [MT03], for  $i = 1, 2, 3, 4$ , we choose a point  $P_i$  of exact order  $\lambda^i$  on  $J$  so that  $\lambda P_i = P_{i-1}$  for  $i = 2, 3, 4$ . These points form a basis for  $J[\lambda^4]$  as a vector space over  $\mathbb{Z}/p\mathbb{Z}$ . Furthermore,  $P_3$  is a  $\lambda^3$ -torsion point, and therefore defined over  $K$ , and  $\lambda$  itself is defined over  $K$ . Therefore, for  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$

$$(2.1) \quad \sigma(P_4) = P_4 - \chi(\sigma)P_1$$

for some isomorphism  $\chi : \text{Gal}(K(\eta_{p-3}^{1/p})/K) \rightarrow \mathbb{Z}/p\mathbb{Z}$ .

**LEMMA 2.2.** *Let  $\chi$  be defined by (2.1). We have a commutative diagram*

$$\begin{array}{ccccccc} 0 & \longrightarrow & J[\lambda] & \longrightarrow & J[\lambda^4] & \xrightarrow{\lambda} & J[\lambda^3] & \longrightarrow & 0 \\ & & \downarrow \simeq & & \downarrow \simeq & & \downarrow \simeq & & \\ 0 & \longrightarrow & \mu_p & \xrightarrow{\iota} & \mu_p^4 & \xrightarrow{\pi} & \mu_p^3 & \longrightarrow & 0 \end{array}$$

in which  $\iota$  is the embedding via the fourth coordinate and  $\pi$  is projection onto the first three coordinates. Furthermore, if we let  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/K)$  act on  $\mu_p^4$  by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \chi(\sigma) & 0 & 0 & 1 \end{pmatrix},$$

and on all other modules in the natural way, then the diagram commutes with the action of  $\text{Gal}(\overline{\mathbb{Q}}/K)$ .

PROOF. For  $i \leq 4$ , let  $e_{\lambda^i}(P, Q)$  be the  $\lambda^i$  Weil pairing on  $J[\lambda^i]$ , as defined, for example, in [McC88]. For any two commuting isogenies  $\phi$  and  $\psi$  of  $J$ , the Weil pairing satisfies

$$e_{\phi}(\psi P, Q) = e_{\phi}(P, \hat{\psi} Q),$$

where  $\hat{\psi}$  is the dual isogeny [McC88, (1.7) and (1.8)]. Define an isomorphism  $J[\lambda^i] \simeq \mu_p^i$  by

$$(2.2) \quad Q \mapsto (e_{\lambda^i}(Q, P_1), \dots, e_{\lambda^i}(Q, P_i)).$$

Our choice of  $P_i$  and  $\chi$  mean that

$$\sigma Q = Q - \chi(\sigma) \lambda^3 Q, \quad Q \in J[\lambda^4].$$

Therefore, if  $1 \leq j \leq i \leq 4$ ,

$$\begin{aligned} e_{\lambda^i}(\sigma Q, P_j) &= e_{\lambda^i}(Q, P_j) - \chi(\sigma) e_{\lambda^i}(\lambda^3 Q, P_j) \\ &= e_{\lambda^i}(Q, P_j) - \chi(\sigma) e_{\lambda^i}(Q, \hat{\lambda}^3 P_j) \\ &= e_{\lambda^i}(Q, P_j) + \chi(\sigma) e_{\lambda^i}(Q, \lambda^3 P_j) \\ &= \begin{cases} e_{\lambda^i}(Q, P_j) + \chi(\sigma) e_{\lambda^i}(Q, P_1) & j = 4 \\ e_{\lambda^i}(Q, P_j) & j < 4. \end{cases} \end{aligned}$$

Here we have used the facts that  $\hat{\lambda} = \bar{\lambda}$ , the complex conjugate of  $\lambda$ , and that  $\bar{\lambda}^3 \equiv -\lambda^3 \pmod{\lambda^4}$ . □

### 3. Selmer Groups

The Selmer group  $S_{\lambda^i}$  is defined by exactness of

$$0 \rightarrow S_{\lambda^i} \rightarrow H^1(K, J[\lambda^i]) \rightarrow \sum_v H^1(K_v, J),$$

where the sum is over a complete set of valuations of  $K$ . We summarize here the basic facts about these Selmer groups, and refer the reader to [McC88] and [MT03] for details.

The isomorphism

$$J[\lambda] \simeq \mu_p$$

chosen in Lemma 2.2 identifies  $S_{\lambda}$  with a subgroup of  $K^{\times}/K^{\times p}$  defined by local conditions at each valuation of  $K$ . For every valuation except the unique  $p$ -adic one, the local condition on  $x \in K^{\times}/K^{\times p}$  is simply that it be a local unit modulo  $p$ -th powers. For the valuation corresponding to the unique prime  $\mathfrak{p}$  of  $K$  above  $p$ , Faddeev calculated the local condition, and found that in the wild non-split and tame cases it is

$$(3.1) \quad x_{\mathfrak{p}} \in 1 + \mathfrak{p}^{(p+3)/2} \mathcal{O}_{\mathfrak{p}} \pmod{K_{\mathfrak{p}}^{\times p}}.$$

(See [Fad61] or [McC88] for the calculation.) Let  $\eta_i \in K^\times/K^{\times p}$  be the element defined by (1.1). By construction it is an eigenvector for the action of  $\text{Gal}(K/\mathbb{Q})$  with character  $\omega^i$ . On the other hand, for  $k \geq 1$ , the action of  $\text{Gal}(K/\mathbb{Q})$  on  $(1 + \mathfrak{p}^k \mathcal{O}_{\mathfrak{p}})/(1 + \mathfrak{p}^{k+1} \mathcal{O}_{\mathfrak{p}})$  is through the character  $\omega^k$ . Thus

$$(3.2) \quad \eta_i \in 1 + \mathfrak{p}^i \mathcal{O}_{\mathfrak{p}} \pmod{K_{\mathfrak{p}}^{\times p}}, \quad 2 \leq i \leq p-3.$$

It follows from (3.1) that  $\eta_i \in S_{\lambda}$  if  $(p+3)/2 \leq i \leq p-3$ . We next show that these elements lift to  $S_{\lambda^3}$ . As before, the local condition at every valuation other than the  $p$ -adic one is that an element be a unit mod  $p$ -th powers in each component. The local condition at  $\mathfrak{p}$  is harder to determine.

For  $i = 1, 2, 3$ , the Galois isomorphisms  $J[\lambda^i] \simeq \mu_p^i$  chosen in Lemma 2.2 identify  $H^1(K, J[\lambda^i])$  with a subgroup of  $(K^\times/K^{\times p})^i$ . It is shown in [MT03, Section 2] that the local descent maps

$$d_k : J(K_{\mathfrak{p}})/pJ(K_{\mathfrak{p}}) \rightarrow H^1(K_{\mathfrak{p}}, J[\lambda^i]) = (K_{\mathfrak{p}}^\times/K_{\mathfrak{p}}^{\times p})^i$$

can be written as

$$d_k = \prod_{j=1}^k \iota_{P_j},$$

where the maps

$$\iota_{P_j} : J(K_{\mathfrak{p}})/pJ(K_{\mathfrak{p}}) \rightarrow K_{\mathfrak{p}}^\times/K_{\mathfrak{p}}^{\times p}$$

are defined by evaluating certain functions  $f_j$  on the curve at divisors representing points on the Jacobian. (The divisor of the function  $f_j$  is  $p$  times a divisor representing the point  $P_j$ .) We have

$$(3.3) \quad \iota_{P_j}(\lambda x) = \iota_{P_{j-1}}(x) \quad \text{for } j = 2, 3.$$

LEMMA 3.1. *If  $C$  has wild non-split or tame reduction and  $\frac{p+5}{2} \leq i \leq p-3$  then the element*

$$(\eta_i, 1, 1) \in (K^\times/K^{\times p})^3$$

*is contained in the Selmer group  $S_{\lambda^3}$ .*

PROOF. Since  $\eta_i$  defines a cocycle which is unramified outside the primes above  $p$ ,  $(\eta_i, 1, 1)$  satisfies all the local conditions for membership in  $S_{\lambda^3}$  except the one at  $\mathfrak{p}$ . Thus membership in  $S_{\lambda^3}$  is equivalent to being in the image of the local descent map at  $\mathfrak{p}$

$$d_3 : J(K_{\mathfrak{p}}) \rightarrow H^1(K_{\mathfrak{p}}, J[\lambda^3]) = (K_{\mathfrak{p}}^\times/K_{\mathfrak{p}}^{\times p})^3.$$

By [MT03, Proposition 4.1] we can choose  $a \in J(K_{\mathfrak{p}})/pJ(K_{\mathfrak{p}})$  such that  $\iota_{P_1}(a) = \eta_i$ , and by applying the necessary idempotent we can suppose that  $a$  is an eigenvector for the action of  $\text{Gal}(K/\mathbb{Q})$ , in which case it is in the  $\omega^i$  eigenspace by [MT03, (4.2)]

Consider  $d_3(a) = (\eta_i, \iota_{P_2}(a), \iota_{P_3}(a))$ . To prove the lemma, we will find  $b \in J(K_{\mathfrak{p}})/pJ(K_{\mathfrak{p}})$  such that  $d_2(b) = (\iota_{P_2}(a)^{-1}, \iota_{P_3}(a)^{-1})$ . Then, by (3.3),

$$d_3(a + \lambda b) = d_3(a) \cdot (1, d_2(b)) = (\eta_i, 1, 1),$$

showing that  $(\eta_i, 1, 1)$  satisfies the local condition at  $\mathfrak{p}$ . Now, Proposition 4.1 and equation (4.2) of [MT03] show that if  $i \geq (p+5)/2$  then

$$\iota_{P_2}(a), \iota_{P_3}(a) \in 1 + \mathfrak{p}^{(p+1)/2} \mathcal{O}_{\mathfrak{p}}.$$

It follows from [MT03, Proposition 4.2] that we can choose  $b \in J(K_{\mathfrak{p}})$  so that  $d_2(b) = (\iota_{P_2}(a)^{-1}, \iota_{P_3}(a)^{-1})$ , as we wanted.  $\square$

#### 4. Proof of Theorem 1.3

Suppose now that we are given  $p$ ,  $r$ , and  $s$  satisfying the conditions of Theorem 1.3. Conditions (1) and (2) imply  $(\eta_{p-r+3}, 1, 1) \in S_{\lambda^3}$ , by Lemma 3.1.

Since  $J$  has good reduction outside  $\mathfrak{p}$  and  $\deg \lambda = p$ , we can regard the Selmer groups  $S_{\lambda^i}$  as subgroups of  $H^1(G, J[\lambda^i])$ , where  $G$  is the Galois group of the maximal extension of  $K$  unramified outside  $\mathfrak{p}$ . Regarding  $(\eta_{p-r+3}, 1, 1)$  as an element of  $H^1(G, J[\lambda^3])$ , we claim that its coboundary in the  $G$ -cohomology of

$$0 \rightarrow J[\lambda] \rightarrow J[\lambda^4] \rightarrow J[\lambda^3] \rightarrow 0$$

is equal to a non-zero multiple of  $\langle \eta_{p-r+3}, \eta_{p-3} \rangle$  under the identification  $H^2(G, J[\lambda]) \simeq H^2(G, \mu_p)$ . This can be seen as follows.

In this paragraph we use additive notation for the abelian group  $\mu_p$ , and we use the diagram and notation of Lemma 2.2. Since  $\mu_p^3$  is fixed by  $G$ , our element  $(\eta_{p-r+3}, 1, 1) \in H^1(G, \mu_p^3)$  is represented by a homomorphism  $(x, 0, 0) : G \rightarrow \mu_p^3$ , which we lift to the cochain

$$\bar{x} = (x, 0, 0, 0) : G \rightarrow \mu_p^4.$$

Then

$$\begin{aligned} \delta(\bar{x})(\sigma, \tau) &= \begin{pmatrix} x(\sigma\tau) \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} x(\sigma) \\ 0 \\ 0 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \chi(\sigma) & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x(\tau) \\ 0 \\ 0 \\ 0 \end{pmatrix} \\ &= - \begin{pmatrix} 0 \\ 0 \\ 0 \\ \chi(\sigma)x(\tau) \end{pmatrix} = \iota_*(-(\chi \cup x)(\sigma, \tau)). \end{aligned}$$

Thus the coboundary is  $-(\chi \cup x)$ , which is equal to  $x \cup \chi$  by skew-symmetry of the cup product on  $H^1$ . Theorem 2.1 implies that  $\chi$  is a non-zero multiple of the Kummer character associated with  $\eta_{p-3}$ . Furthermore,  $x$  is the Kummer character associated with  $\eta_{p-r+3}$ . Hence, under condition (3), the coboundary is nontrivial.

Finally, non-triviality of the coboundary implies non-triviality in III by virtue of the commutative diagram with exact rows and columns:

$$\begin{array}{ccccc} J(K)/\lambda^4 J(K) & \longrightarrow & J(K)/\lambda^3 J(K) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow \\ S_{\lambda^4} & \xrightarrow{\lambda_*} & S_{\lambda^3} & \xrightarrow{\delta} & H^2(G, J[\lambda]) \\ & & \downarrow & & \\ & & \text{III} & & \end{array}$$

This concludes the proof of the theorem.

#### 5. Concluding remarks

From consideration of the action of  $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ , one does not expect often any overlap between the non-trivial elements of III produced by Theorems 1.1, 1.2 and 1.3. Furthermore, in many cases we can increase a lower bound on the order

of  $\text{III}$  using the following result, which depends on showing the triviality in many cases of the Cassels pairing between  $\text{III}[\lambda^2]$  and  $\text{III}[\lambda]$ .

**THEOREM 5.1.** [**MT03**, Theorem 1.2] *Suppose that  $F_s$  is wild non-split or tame and either  $p \equiv 1 \pmod{4}$  and  $p \nmid B_{(p-1)/2}$ , or  $p \equiv 3 \pmod{4}$  and  $p \nmid B_{(p-3)/2}$ . Then  $\text{III}[\lambda^2]/\lambda\text{III}[\lambda^3] = 0$ , that is,  $\text{III}[\lambda^3]$  is a free module over  $\mathbb{Z}[\zeta]/(\lambda^3)$ .*

Thus, for example, in the case of the curve  $y^{691} = x(1-x)$  mentioned in Section 1, where we found that  $\text{III}$  contains a subgroup isomorphic to  $\mathbb{Z}/691\mathbb{Z}$ , Theorem 5.1 implies, combined with eigenspace considerations, implies that it contains a subgroup isomorphic to  $(\mathbb{Z}/691\mathbb{Z})^3$ . A survey of small irregular primes produces many more examples with large subgroups of  $\text{III}$ . For the curves studied here it seems to be much easier to find elements in  $\text{III}$  than elements of the Mordell-Weil group.

### References

- [Fad61] D. K. Faddeev, *Invariants of divisor classes for the curves  $x^k(1-x) = y^l$  in an  $l$ -adic cyclotomic field*, Trudy Mat. Inst. Steklov. **64** (1961), 284–293.
- [GR78] Benedict H. Gross and David E. Rohrlich, *Some results on the Mordell-Weil group of the jacobian of the Fermat curve*, Invent. Math. **44** (1978), 201–224.
- [Gre81] Ralph Greenberg, *On the Jacobian variety of some algebraic curves*, Compositio Math. **42** (1980/81), no. 3, 345–359.
- [McC88] William G. McCallum, *On the Shafarevich-Tate group of the Jacobian of a quotient of the Fermat curve*, Invent. Math. **93** (1988), no. 3, 637–666.
- [McC92] William McCallum, *The arithmetic of Fermat curves*, Math. Ann. **294** (1992), 503–511.
- [MS03] William G. McCallum and Romyar T. Sharifi, *A cup product in the Galois cohomology of number fields*, Duke Math. J. **120** (2003), no. 2, 269–310. MR MR2019977 (2004j:11136)
- [MT03] William G. McCallum and Pavlos Tzermias, *On Shafarevich-Tate groups and the arithmetic of Fermat curves*, Number theory and algebraic geometry, London Math. Soc. Lecture Note Ser., vol. 303, Cambridge Univ. Press, Cambridge, 2003, pp. 203–226.
- [Sha07] Romyar T. Sharifi, *Iwasawa theory and the Eisenstein ideal*, Duke Math. J. **137** (2007), no. 1, 63–101.
- [Was97] Lawrence Washington, *Introduction to cyclotomic fields*, 2nd ed., Springer-Verlag, New York, 1997.

DEPARTMENT OF MATHEMATICS, CALIFORNIA STATE UNIVERSITY, CHICO, CA 95929, USA  
*E-mail address:* benjamin.levitt@gmail.com

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ARIZONA, TUCSON, AZ 85718, USA  
*E-mail address:* wmc@math.arizona.edu  
*URL:* http://math.arizona.edu/~wmc