On Shafarevich–Tate groups and the arithmetic of Fermat curves

William G. McCallum Pavlos Tzermias

To Sir Peter Swinnerton-Dyer on his 75th birthday.

1 Introduction

Let $\mathbb{Q}$ denote the field of rational numbers and $\overline{\mathbb{Q}}$ a fixed algebraic closure of $\mathbb{Q}$. For a fixed prime p such that $p \geq 5$, choose a primitive pth root of unity ζ in $\overline{\mathbb{Q}}$ and let $K = \mathbb{Q}(\zeta)$. If a, b and c are integers such that $0 < a, b, a+b < p$ and $a + b + c = 0$, let $F_{a,b,c}$ denote a smooth projective model of the affine curve

$$y^p = x^a(1-x)^b \tag{1.1}$$

and let $J_{a,b,c}$ be the Jacobian of $F_{a,b,c}$. Then $J_{a,b,c}$ has complex multiplication induced by the birational automorphism $(x, y) \mapsto (x, \zeta y)$ of $F_{a,b,c}$. Let λ denote the endomorphism $\zeta - 1$ of $J_{a,b,c}$. Note that λ^{p-1} is, up to a unit in $\mathbb{Z}[\zeta]$, multiplication by p on $J_{a,b,c}$.

We are interested in the Shafarevich–Tate group of $J_{a,b,c}$ over K, which we denote simply by Ш. In [McC88], the first author studied the restriction of the Cassels–Tate pairing

$$Ш[\lambda] \times Ш[\lambda] \longrightarrow \mathbb{Q}/\mathbb{Z} \tag{1.2}$$

and showed that $Ш[\lambda]$ is nontrivial in certain cases depending on the reduction type of the minimal regular model of $F_{a,b,c}$ over $\mathbb{Z}_p[\zeta]$. The purpose of this paper is to extend those results by carrying out higher descents, and to derive some consequences for the arithmetic of Fermat curves using the techniques of the second author.

First we recall the main result of [McC88]. The possible reduction types for $F_{a,b,c}$ are as shown in Figure 1 [McC82], with the proper transform of the special fiber of the model (1.1) indicated. The wild type is further divided into split and nonsplit, according to whether the two tangent components are

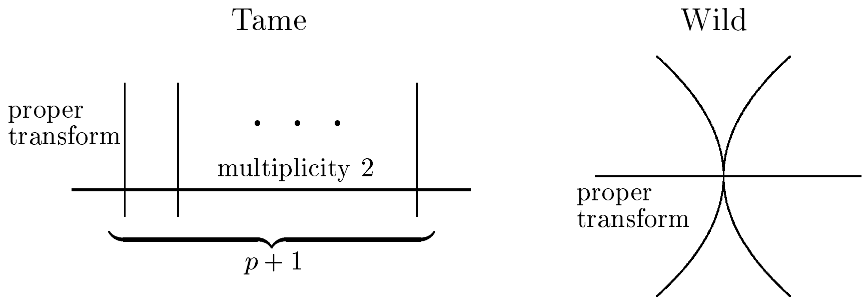

Figure 1: Reduction types of $F_{a,b,c}$

defined over the finite field $\mathbb{F}_p$ or conjugate over a quadratic extension. The reduction type can be computed as follows. For a rational number x of p-adic valuation 0, let $q(x) = (x^{p-1} - 1)/p$, viewed as an element of $\mathbb{F}_p$. Then $F_{a,b,c}$ is

$$\begin{cases} \text{tame} & \text{if } -2abcq(a^a b^b c^c) = 0, \\ \text{wild split} & \text{if } -2abcq(a^a b^b c^c) \in \mathbb{F}_p^{\times 2}, \\ \text{wild nonsplit} & \text{if } -2abcq(a^a b^b c^c) \notin \mathbb{F}_p^{\times 2}. \end{cases}$$

Let M_K be the set of finite places of K and let w denote the unique place of K above p. Define

$$\begin{aligned} U &= \left\{x \in K^\times/K^{\times p} : v(x) \equiv 0 \pmod{p} \text{ for all } v \in M_K\right\}, \\ V &= K_w^\times/K_w^{\times p}. \end{aligned} \tag{1.3}$$

Let π be the uniformizer of K_w defined by

$$\pi^{p-1} = -p \quad \text{and} \quad \frac{\pi}{1-\zeta} \equiv 1 \pmod{w}. \tag{1.4}$$

If $\kappa\colon \mathrm{Gal}(K/\mathbb{Q}) \to \mathbb{Z}_p^\times$ is the Teichmüller character, let $V(i)$ denote the intersection of the κ^ith eigenspace of V with the subgroup of V generated by units congruent to 1 modulo π^i. Thus $V(i)$ is one-dimensional if $2 \leq i \leq p$.

Theorem 1.1 ([McC88]) *Suppose that $F_{a,b,c}$ is wild split, $p \equiv 1 \pmod{4}$, and the image of U is nontrivial in both $V((p-1)/2)$ and $V((p+3)/2)$. Then*

$$Ш[\lambda]/\lambda Ш[\lambda^2] \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}.$$

The condition on U is satisfied if $p \nmid B_{(p-1)/2}B_{(p+3)/2}$, where B_k is the kth Bernoulli number. As noted in [McC88], the technique used to prove Theorem 1.1 applies to the pairing

$$Ш[\lambda^2] \times Ш[\lambda] \longrightarrow \mathbb{Q}/\mathbb{Z} \tag{1.5}$$

and yields information about $Ш[\lambda^2]$.

Theorem 1.2 *Suppose that either of the following conditions is satisfied:*

(a) $F_{a,b,c}$ *is wild split and* $p \equiv 3 \pmod 4$*;*

(b) $F_{a,b,c}$ *is wild nonsplit or tame and the image of* U *in either* $V((p+1)/2)$ *or* $V((p+3)/2)$ *is trivial.*

Then the pairing (1.5) *is trivial. Thus* $Ш[\lambda^2]/\lambda Ш[\lambda^3] = 0$*, that is,* $Ш[\lambda^3]$ *is a free module over* $\mathbb{Z}[\zeta]/(\lambda^3)$*.*

As discussed in [McC88], the hypothesis on U in condition (b) of the theorem is quite mild, since for U to be nontrivial in $V(k)$ with $k > 1$ and odd requires that p divides B_{p-k}.

Corollary 1.3 *If one of conditions (a) or (b) of Theorem 1.2 is satisfied, and if* $|Ш[p^\infty]| < p^3$*, then* $Ш[p^\infty] = 0$*.*

Under the conditions of Theorem 1.2, it is natural to ask which occurs more often: $|Ш[p]| = 0$ or $|Ш[p]| \geq p^3$. To explore this question, we compute

$$Ш[\lambda^3] \times Ш[\lambda] \longrightarrow \mathbb{Q}/\mathbb{Z}. \tag{1.6}$$

Theorem 1.4 *Suppose that* $p \geq 19$ *is regular,* $p \equiv 3 \pmod 4$*,* $F_{a,b,c}$ *is tame or wild nonsplit and*

$$q(a^a b^b c^c)^3 + abcB_{p-3} \not\equiv 0 \pmod p. \tag{1.7}$$

Then the pairing (1.6) *is nontrivial. Thus* $Ш[\lambda^3] \neq 0$ *(and hence, by Corollary 1.3,* $|Ш[p^\infty]| \geq p^3$*).*

For example, the curve $y^{19} = x^2(1-x)$ satisfies the conditions of the theorem. Modest numerical experiments suggest that about half the curves satisfy the conditions. More precisely, there are about $p/6$ isomorphism classes of curves $F_{a,b,c}$ for a given prime p, and heuristically about half of them are tame or wild nonsplit. The incongruence (1.7) is usually satisfied for these curves; for example, it is satisfied for all such curves if $p < 100$ (and $p \equiv 3 \pmod 4$).

The next result shows that, in certain cases, one can combine Theorems 1.2 and 1.4 to describe the exact structure of $Ш[p^\infty]$:

Theorem 1.5 *Suppose that* p*,* a*,* b *and* c *are chosen to satisfy the hypotheses of both Theorems 1.2 and 1.4. If, in addition, the free* $\mathbb{Z}[\zeta]/(\lambda^3)$*-module* $Ш[\lambda^3]$ *has rank* 2*, then*

$$Ш[p^\infty] = Ш[\lambda^3] \simeq (\mathbb{Z}[\zeta]/(\lambda^3))^2.$$

In Section 6 we establish the following application of the above results:

Theorem 1.6 *Let $p = 19$, $a = 7$, $b = 1$. Then*

1. $Ш[p^\infty] \simeq (\mathbb{Z}[\zeta]/(\lambda^3))^2$.
2. *The Mordell–Weil rank of $J_{7,1,-8}$ over $\mathbb{Q}$ equals* 1.
3. *The only quadratic points (i.e. algebraic points whose field of definition is a quadratic extension of $\mathbb{Q}$) on the Hurwitz–Klein curve $F_{7,1,-8}$ and also on the Fermat curve $X^{19} + Y^{19} + Z^{19} = 0$ are those described by Gross and Rohrlich in [GR78].*

We also note that, by combining Theorem 1.4 with Faddeev's bounds in [Fad61], one gets that the Mordell–Weil rank (over $\mathbb{Q}$) of any tame or wild nonsplit quotient of the Fermat curve F_{19} or F_{23} is at most 2.

Lim [Lim95] has also stated a result attempting to improve on [McC88] in certain cases. However, in Section 6, we show that the hypotheses of Propositions A and B of [Lim95] are never simultaneously satisfied.

2 Formulas for the pairings

We recall the situation and notation of [McC88]. For $\phi \in \mathcal{O}_K$ and F a field containing K, we write $\delta = \delta_{\phi,F}$ for the coboundary map $J(F) \to H^1(F, J[\phi])$. The ϕ-Selmer group $S_\phi \subset H^1(K, J[\phi])$ is defined to be the subgroup whose specialization to each completion K_v of K lies in the image of δ_{ϕ,K_v}. It sits in an exact sequence

$$0 \to J(K)/\phi J(K) \to S_\phi \to Ш[\phi] \to 0.$$

For $\phi, \psi \in \mathrm{End}(J)$, we have a pairing

$$S_\phi \times S_{\hat{\psi}} \to \mathbb{Q}/\mathbb{Z}, \tag{2.1}$$

described in [McC88], which is a lift of the restriction of the Cassels pairing to $Ш[\phi] \times Ш[\hat{\psi}]$. An expression for the pairing (2.1) is given in [McC88], under a certain splitting hypothesis.

We use[McC88] to derive formulas for the pairings (1.5) and (1.6). The formula for (1.5) is a straightforward consequence of Theorem 2.6 in [McC88]; the formula for (1.6) takes more work. The point is that $J[\lambda^3] \subset J(K)$ (Greenberg [Gre81]), so that it is possible to express the pairings (1.2) and (1.5) as purely local pairings at w, as explained in [McC88]. However, by [Gre81] and Kurihara [Kur92], the λ^4-torsion on $J_{a,b,c}$ is not in general defined over K, introducing an essentially global aspect to the calculation of (1.6).

For technical reasons, it is convenient to replace λ with an endomorphism (which we also denote by λ) that is congruent modulo λ^5 to the uniformizer π defined by (1.4), since then

$$\lambda^\delta \equiv \kappa(\delta)\lambda \pmod{\lambda^5}, \quad \delta \in \mathrm{Gal}(K/\mathbb{Q}).$$

In particular, we have $\hat{\lambda} \equiv -\lambda$ modulo λ^5, and we will often replace $\hat{\lambda}$ with $-\lambda$ without mention in what follows, in cases where we are dealing with a module killed by λ^5. Furthermore, it suffices to prove Theorems 1.2 and 1.4 with this new choice of λ. Since $\lambda/\hat{\lambda}$ is a unit, $Ш[\lambda] = Ш[\hat{\lambda}]$, and we can proceed by computing the pairing $\langle\ ,\ \rangle_k$ mentioned in (2.1) with $\phi = \lambda^k$ and $\psi = \hat{\lambda}$.

The local formula for the Cassels–Tate pairing is expressed in terms of certain local descent maps as follows. Given a p-torsion point Q in $J(\overline{K})$ we denote by D_Q a divisor defined over $K(Q)$ representing Q and by f_Q a function on $F_{a,b,c}$ whose divisor is pD_Q. Evaluating f_Q on divisors induces a map $\iota_Q\colon J(F) \to F^\times/F^{\times p}$ for any field F containing $K(Q)$.

By [Gre81],

$$K(J[\lambda^3]) = K \quad \text{and} \quad K(J[\lambda^4]) = L = K(\eta_{p-3}^{1/p}), \tag{2.2}$$

where η_{p-3} is a generator for the κ^{p-3}-eigenspace of the cyclotomic units in K. Let $\tilde{\Delta} \subset \mathrm{Gal}(L/\mathbb{Q})$ be a subgroup projecting isomorphically to $\mathrm{Gal}(K/\mathbb{Q})$. For $i = 1, 2, 3, 4$, we choose points P_i of order λ^i on J and a generator σ for $G = \mathrm{Gal}(L/K)$ such that

1. P_1 is the point represented by the divisor $(0, 0) - \infty$;
2. $\lambda P_i = P_{i-1}$ for $i = 2, 3, 4$;
3. P_i is an eigenvector for the action of $\tilde{\Delta}$ with character κ^{1-i};
4. $\sigma P_4 = P_4 + P_1$.

For $i \leq 4$, let $e_{\lambda^i}(P, Q)$ be the λ^i Weil pairing on $J[\lambda^i]$. We have an isomorphism $J[\lambda^i] \simeq \mu_p^i$ defined over $K(P_i)$ (and thus over K for $i \leq 3$), given by

$$Q \mapsto (e_{\lambda^i}(Q, P_1), \ldots, e_{\lambda^i}(Q, P_i)). \tag{2.3}$$

With this identification, by [McC88, Lemma 2.2], we have

$$\delta_i = \delta_{\lambda^i, K(P_i)} = \iota_{P_1} \times \cdots \times \iota_{P_i}.$$

Since J has good reduction outside p and λ has degree p, we can regard S_{λ^i} as a subgroup of $H^1(K(p)/K, J[\lambda^i])$, where $K(p)/K$ is the maximal extension of K unramified outside p. As explained in Section 7 of [McC88], we can also regard S_{λ^i} as a subgroup of U^i for $i \leq 3$, where U is as defined in (1.3). For $a, b \in K_w^\times$, denote by (a, b) the Hilbert symbol.

Proposition 2.1 *Let $a \in S_{\lambda^2}$, $b \in S_{\hat{\lambda}}$, $a_w = \delta(x_w)$, $x_w \in J(K_w)$. Then*

$$\zeta^{p\langle a,b\rangle_2} = (\iota_{P_3}(x_w), b_w).$$

Proof This follows from [McC88, Theorem 2.6], with $\phi = \lambda^2$ and $\psi = \lambda$. □

For a number field F we denote by $\mathcal{O}'_F$ the ring of p-integers in F. Suppose $F \subset K(p)$ and let C be the ideal class group of $\mathcal{O}'_F$. Since the group $\mathcal{O}'^{\times}_{K(p)}$ is p-divisible, we have an exact sequence

$$0 \to \mu_p \to \mathcal{O}'^{\times}_{K(p)} \xrightarrow{p} \mathcal{O}'^{\times}_{K(p)} \to 0,$$

which induces a long exact sequence of Galois cohomology

$$\begin{gathered} \cdots \to H^{i-1}(K(p)/F, \mathcal{O}'^{\times}_{K(p)}) \xrightarrow{p} H^{i-1}(K(p)/F, \mathcal{O}'^{\times}_{K(p)}) \to \\ H^{i}(K(p)/F, \mu_p) \to H^{i}(K(p)/F, \mathcal{O}'^{\times}_{K(p)}) \xrightarrow{p} H^{i}(K(p)/F, \mathcal{O}'^{\times}_{K(p)}) \to \cdots \end{gathered}$$

If $i = 1$ then, since $H^1(K(p)/F, \mathcal{O}'^{\times}_{K(p)})$ is isomorphic to C, we obtain the exact sequence

$$0 \to \mathcal{O}'^{\times}_F/\mathcal{O}'^{\times p}_F \to H^1(K(p)/F, \mu_p) \to C[p] \to 0. \tag{2.4}$$

Also, by [NSW00, VIII.3], it follows that $H^2(K(p)/F, \mathcal{O}'^{\times}_{K(p)})[p^\infty]$ can be identified with the subgroup $\mathrm{Br}(K(p)|F)[p^\infty]$ of $\mathrm{Br}(F)[p^\infty]$. Setting $i = 2$ in the above long exact cohomology sequence gives another exact sequence

$$0 \to C/pC \to H^2(K(p)/F, \mu_p) \to \mathrm{Br}(K(p)/F)[p] \to 0. \tag{2.5}$$

Lemma 2.2 *Every element of $H^1(K(p)/K, J[\lambda^k])$ lifts to $H^1(K, J[\lambda^{k+1}])$. Moreover, if p is regular, it lifts to $H^1(K(p)/K, J[\lambda^{k+1}])$.*

Proof Let $a \in H^1(K(p)/K, J[\lambda^k])$, and let $\delta a \in H^2(K(p)/K, J[\lambda])$ be the coboundary of a for the sequence

$$0 \to J[\lambda] \to J[\lambda^{k+1}] \to J[\lambda^k] \to 0. \tag{2.6}$$

Then the inflation of δa in $H^2(K, J[\lambda]) \simeq H^2(K, \mu_p) = \mathrm{Br}(K)[p]$ has zero invariant at every place not dividing p. Thus it is zero by the Brauer–Hasse–Noether theorem (since there is only one place of K dividing p). For the second statement, we argue in the same way, using (2.5). □

We recall the definition of $\langle\ ,\ \rangle_3$. Let $a \in S_{\lambda^3}$ and $b \in S_{\hat{\lambda}}$. Lift a to an element a_1 of $H^1(K, J[\lambda^4])$ (which is possible by Lemma 2.2). For each place

v of K, lift a_v to an element $a_{v,1}$ that is in the image of δ. Then $a_{1,v} - a_{v,1}$ is the image of an element $c_v \in H^1(K_v, J[\lambda])$, and

$$\langle a, b\rangle = \sum_v c_v \cup b_v$$

where the cup product is with respect to the local pairing

$$H^1(K_v, J[\lambda]) \times H^1(K_v, J[\hat{\lambda}]) \to \mathbb{Q}/\mathbb{Z}.$$

If p is regular, L/K is totally ramified at w, and there is a unique extension of w to L, that we also denote by w. Let $N' = \sum_{i=1}^{p-1} i\sigma^i$.

Proposition 2.3 *Let $a \in S_{\lambda^3}$, $b \in S_\lambda$, $a_w = \delta(x_w)$, $x_w \in J(K_w)$. Suppose that $\lambda_*^2 a$, regarded as an element of $\mathcal{O}_K^\times/\mathcal{O}_K^{\times p}$, can be written as $N_{L/K}\epsilon$ for some $\epsilon \in \mathcal{O}_L^\times$. Then there exists a λ^4-torsion point P_4, and an element $c_w \in K_w^\times$ such that*

$$\zeta^{p\langle a,b\rangle_3} = (c_w, b_w),$$

and the image of c_w in $L_w^\times/L_w^{\times p}$ satisfies

$$c_w = \iota_{P_4}(x_w)^{-1}\eta N'\epsilon,$$

where $\eta \in H^1(K(p)/L, \mu_p)^G$. In addition, if a and b are eigenvectors for the action of Δ, we may assume that c_w is also.

Proof Consider the sequence

$$0 \to J[\lambda] \to J[\lambda^4] \to J[\lambda^3] \to 0 \tag{2.7}$$

and the commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 \to & H^1(K(p)/L, J[\lambda])^G & \longrightarrow & H^1(K(p)/L, J[\lambda^4])^G & \xrightarrow{\lambda_*} & H^1(K(p)/L, J[\lambda^3])^G \\ & {\scriptstyle \mathrm{res}_{L/K}}\uparrow & & {\scriptstyle \mathrm{res}_{L/K}}\uparrow & & {\scriptstyle \mathrm{res}_{L/K}}\uparrow \\ & H^1(K(p)/K, J[\lambda]) & \longrightarrow & H^1(K(p)/K, J[\lambda^4]) & \xrightarrow{\lambda_*} & H^1(K(p)/K, J[\lambda^3]). \end{array}$$

The top row is exact because (2.7) splits over L, and hence the sequence

$$0 \to H^1(K(p)/L, J[\lambda]) \to H^1(K(p)/L, J[\lambda^4]) \to H^1(K(p)/L, J[\lambda^3])$$

is exact. By Lemma 2.2, a lifts to an element $a_1 \in H^1(K(p)/K, J[\lambda^4])$. Let $a_1' \in H^1(K(p)/L, J[\lambda^4])^G$ be any lift of $\mathrm{res}_{L/K}\, a$ ($\mathrm{res}_{L/K}\, a_1$ itself is one such). Then

$$\mathrm{res}_{L/K}\, a_1 = a_1'\eta \quad \text{and} \quad \eta \in H^1(K(p)/L, \mu_p)^G. \tag{2.8}$$

We now construct a candidate for a_1'. Under the identification (2.3) between $J[\lambda^i]$ and μ_p^i, the map $\lambda^{i-1} : J[\lambda^i] \to J[\lambda]$ corresponds to projection on the first component. Hence under the identification $H^1(K, J[\lambda^3]) = (K^\times/K^{\times p})^3$, a corresponds to an element $(x_1, x_2, x_3) \in (K^\times/K^{\times p})^3$, and $\lambda_*^2 a = x_1$. Moreover, in the identification

$$H^1(L, J[\lambda^4]) \simeq (L^\times/L^{\times p})^4,$$

the action of σ on $H^1(L, J[\lambda^4])$ is intertwined with

$$(t_1, t_2, t_3, t_4) \mapsto (t_1^\sigma, t_2^\sigma, t_3^\sigma, t_4^\sigma t_1^\sigma), \quad t_i \in L^\times/L^{\times p}.$$

Thus (t_i) is fixed by G if

$$t_i^\sigma = t_i, \quad i = 1, 2, 3, \quad \text{and} \quad t_4^{\sigma-1} = t_1^{-1}.$$

By hypothesis, $x_1 = N_{L/K}\epsilon$, $\epsilon \in \mathcal{O}_L^\times$. Then

$$a_1' = (x_1, x_2, x_3, N'\epsilon) \tag{2.9}$$

is an equivariant lift of (x_1, x_2, x_3).

Now let $a_{w,1}$ be the local lift of a given by $a_{w,1} = \delta_4(x_w)$. Then

$$\operatorname{res}_{L_w/K_w} a_{w,1} = (x_1, x_2, x_3, \iota_{P_4}(x_w)). \tag{2.10}$$

Thus, from equations (2.8), (2.9), and (2.10), we get

$$\operatorname{res}_{L_w/K_w}(c_w) = \operatorname{res}_{L_w/K_w}(a_{1,w} - a_{w,1}) = \iota_{P_4}(x_w)^{-1}\eta N'\epsilon.$$

The last statement of the proposition is clear, since at each stage in the calculation we can choose eigenvectors, and the maps λ and ι_{P_k} are also eigenvectors for the action of Δ, by the choices we have made of λ and P_k. □

3 The local approximation

Let P_i be as in the previous section, $i = 1, 2, 3, 4$, let D_i be a divisor on $F_{a,b,c}$ representing P_i, and let f_i be a function whose divisor is pD_i. Take D_i and f_i to be defined over $K = \mathbb{Q}(\zeta)$ if $i = 1, 2, 3$ and over $L = K(\eta_{p-3}^{1/p})$ if $i = 4$. The maps ι_{P_i} in Propositions 2.1 and 2.3 are computed by evaluating f_i on certain divisors. We use the approximation technique in [McC88] to find expansions for f_i on p-adic discs in $F_{a,b,c}$. Given a function f whose divisor is divisible by p we approximate f on an affinoid Y in $F_{a,b,c}$ using the fact that

$$\frac{df}{f} \equiv \omega \quad (\operatorname{mod}_Y p). \tag{3.1}$$

for some holomorphic differential ω on $F_{a,b,c}$ ([McC88], Theorem 5.2). For general facts about rigid analysis, we refer the reader to [BGR84].

We recall the notion of congruence used in (3.1). If Y is a one-dimensional affinoid defined over an extension F of $\mathbb{Q}_p$ with uniformizer π_F, we let $A(Y)$ be the ring of rigid analytic functions on Y, $M(Y)$ the quotient field of $A(Y)$, and $D(Y)$ the module of Kähler differentials of $M(Y)$. We define sub-$\mathcal{O}_F$-modules

$$\begin{aligned} A^0(Y) &= \{f \in A(Y) : |f(x)| \leq 1 \text{ for all } x \in Y(\mathbb{C}_p)\} \\ M^0(Y) &= \{f/g : f \in A^0(Y), g \in A^0(Y) \setminus \pi_F A^0(Y)\} \\ D^0(Y) &= \{\sum_i f_i\, dg_i : f_i, g_i \in M^0(Y)\}. \end{aligned}$$

If $f, g \in A(Y)$, $c \in F$, we say that $f \equiv g \pmod{_Y\, c}$ if $(f-g) \in cA^0(Y)$, and similarly we define the notion of congruence on Y in $M(Y)$ and $D(Y)$. In order to deduce from (3.1) information about power series expansions of f on closed discs in Y, we need the following lemmas.

Lemma 3.1 *Suppose that Y is a one-dimensional affinoid over a finite extension F of $\mathbb{Q}_p$, Y has good reduction, and Z is an affinoid contained in Y, isomorphic to a closed disc. If $\omega \in D^0(Y)$ is a differential with at worst simple poles on Y that is regular on Z, then $\omega \in D^0(Z)$.*

Proof Since Z is isomorphic to a closed disc, it is contained in a residue class U of Y (or is equal to Y, in which case there is nothing to prove). It is clear from the definitions that $D^0(Y)|_U = D^0(U)$, hence $\omega \in D^0(U)$. Furthermore, since Y has good reduction, U is isomorphic to an open disc. Choose a parameter t for U such that Z is the disc $|t| \leq |c| < 1$ for some $c \in F$, and write

$$\omega = g\, dt + \sum_{i=1}^{n} \frac{a_i}{t - b_i}\, dt, \quad g \in \mathcal{O}_F[[t]], \quad a_i, b_i \in \mathcal{O}_F, \quad |c| < |b_i| < 1.$$

Expanding the polar terms in powers of t/b_i and setting $t = cs$, we get $\omega = f\, ds$ for some $f \in \mathcal{O}_F[[s]]$. Since s is a parameter on Z, this proves the lemma. $\square$

Lemma 3.2 *Suppose that f is a function whose divisor is divisible by p. Let Y be an affinoid with good reduction contained in $F_{a,b,c}$ and let Z be a p-adic disc contained in Y such that there is a function on $F_{a,b,c}$ restricting to a parameter on Z. If ω satisfies the congruence (3.1)* $(\mathrm{mod}_Y\ p)$*, then it satisfies the same congruence* $(\mathrm{mod}_Z\ p)$.

Proof With notation as in [McC88], we have

$$\frac{df}{f} = \omega + p\eta, \quad \eta \in D^0(Y).$$

Let g be a function on $F_{a,b,c}$ such that f/g^p is regular on Z (we can construct g using a parameter on Z as in the hypotheses). Since a suitable scalar multiple of g is in $M^0(Y)$, $d\log g \in D^0(Y)$. Thus $\eta - d\log g \in D^0(Y)$ and is also regular on Z, and hence is in $D^0(Z)$ by Lemma 3.1. Thus

$$\frac{df}{f} \equiv \frac{df}{f} - p\frac{dg}{g} = \omega + p\Big(\eta - \frac{dg}{g}\Big) \equiv \omega \quad (\mathrm{mod}_Z\ p). \quad \square$$

We apply these considerations to the affinoid Y introduced in [McC88] and defined as follows. Choose $\pi_K = \pi$ as the uniformizer for K_w. Let s and t be the functions on $F_{a,b,c}$ defined by

$$x = -\frac{a}{c}(1 + \pi^{(p-1)/2}s) \tag{3.2}$$
$$y = (-1)^c a^a b^b c^c (1 + \pi t). \tag{3.3}$$

Let Y be the affinoid defined over L_w by the inequalities

$$|t| \le |\pi_L^{-1}|, \quad |s| \le 1.$$

A basis of holomorphic differentials on $F_{a,b,c}$ is

$$\omega_k = E_k \frac{x^{\left[\frac{ka}{p}\right]}(1-x)^{\left[\frac{kb}{p}\right]}}{y^k}\, dx, \quad k \in H_{a,b,c},$$

for some constants E_k and where $H_{a,b,c}$ is a certain subset of $\{1, 2, \ldots, p-1\}$ of cardinality $(p-1)/2$ (we can identify $H_{a,b,c}$ with the CM-type of $F_{a,b,c}$). We can and do choose the constants E_k so that ω_k has expansion

$$\omega_k \equiv ds \quad (\mathrm{mod}_Y\ \pi_L), \tag{3.4}$$

(note that this normalization is different from that of [McC88]). Now P_1 is the λ-torsion point represented by the divisor $(0,0) - \infty$, and we choose $f_1 = x$. In [McC88] it was shown that

$$\frac{df_1}{f_1} \equiv \pi^{(p-1)/2} \sum_{k \in H_{a,b,c}} b_k \omega_k \quad (\mathrm{mod}_Y\ p) \tag{3.5}$$

for some p-adic integers b_k satisfying

$$\sum_{k \in H_{a,b,c}} b_k k^i \equiv \begin{cases} F & i = 0 \\ 0 & 1 \le i \le (p-3)/2 \end{cases} \quad (\mathrm{mod}\ \pi_K), \quad F \in \mathbb{Z}/p\mathbb{Z}^\times. \tag{3.6}$$

Note that although it was assumed that $F_{a,b,c}$ is wild split in Section 5 of [McC88], there is nothing in the definition of Y or the calculation showing (3.5) and (3.6) that uses this assumption. It is only at the end of that section that the assumption comes in.

Lemma 3.3 *If*

$$\sum_{k\in H_{a,b,c}} u_k\omega_k \equiv \sum_{k\in H_{a,b,c}} v_k\omega_k \pmod{_Y\ \pi^{n+(p-3)/2}}$$

then

$$u_k \equiv v_k \pmod{\pi^n}, \quad k \in H_{a,b,c}.$$

Proof See pages 658–659 of [McC88]. $\square$

Proposition 3.4 *We have*

$$\frac{df_3}{f_3} \equiv \sum_{k\in H_{a,b,c}} c_k\omega_k \pmod{_Y\ p}, \quad c_k \equiv 0 \pmod{\pi^{(p-5)/2}}$$

and

$$\frac{df_4}{f_4} \equiv \sum_{k\in H_{a,b,c}} d_k\omega_k \pmod{_Y\ p}, \quad d_k \equiv -\pi^{(p-7)/2}\frac{b_k}{k^3} \pmod{\pi^{(p-5)/2}}, \tag{3.7}$$

where the b_k are as in equation (3.5).

Proof We have

$$\lambda_*^2\frac{df_3}{f_3} \equiv \frac{df_1}{f_1} \pmod{_Y\ p}.$$

Since $\zeta_*\omega_k = \zeta^{-k}\omega_k$, we have $\lambda_*\omega_k = \lambda^\sigma\omega_k$, for some $\sigma \in \mathrm{Gal}(K_w/\mathbb{Q}_p)$. Hence it follows from Lemma 3.3 and (3.5) that

$$\lambda^{2\sigma}c_k \equiv \pi^{(p-1)/2}b_k \pmod{\pi^{(p+1)/2}}.$$

Thus $c_k \equiv 0 \pmod{\pi^{(p-5)/2}}$, as claimed. Similarly, we have $\lambda_*^3(df_4/f_4) \equiv (df_1/f_1)$, so $\lambda^{3\sigma}d_k \equiv \pi^{(p-1)/2}b_k \pmod{\pi^{(p+1)/2}}$. Furthermore, since $\zeta^\sigma = \zeta^{-k}$, it follows from our choice of λ that $\lambda^\sigma/\pi \equiv -k \pmod{\pi}$ for $1 \le k \le p-1$, so we get equation (3.7). $\square$

Lemma 3.5

$$-\sum_{k\in H_{a,b,c}} \frac{b_k}{k^3} \equiv F(q(a^ab^bc^c)^3 + abcB_{p-3}) \pmod{\pi},$$

where F is as in (3.6).

Proof Let $n = (p-1)/2$. Define

$$\Gamma_k(x_1, \ldots, x_n) = \det \begin{bmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^{n-2} & x_2^{n-2} & \ldots & x_n^{n-2} \\ x_1^{n-1+k} & x_2^{n-1+k} & \ldots & x_n^{n-1+k} \end{bmatrix}.$$

Then an elementary linear algebra calculation using (3.6) gives

$$\sum_{k \in H_{a,b,c}} \frac{b_k}{k^3} \equiv F\Gamma_3(H_{a,b,c}^{-1})/\Gamma_0(H_{a,b,c}^{-1}) \pmod{\pi}.$$

Let $S_i(x_1, \ldots, x_n)$ be the ith symmetric function. Then

$$\Gamma_3 = \Gamma_0(S_1^3 - 2S_1S_2 + S_3).$$

This can be proved by the usual method: the determinant vanishes if $x_i = x_j$ for $i \neq j$, or if there is a polynomial of degree $n+2$ vanishing on the x_i, and with no term of degree $n-1$, n, or $n+1$. Thus, if the roots of the polynomial are $x_1, \ldots, x_n, \alpha, \beta$, then

$$\begin{aligned} \alpha + \beta + S_1 &= 0, \\ S_2 + (\alpha+\beta)S_1 + \alpha\beta &= 0, \\ \alpha\beta S_1 + \alpha S_2 + \beta S_2 + S_3 &= 0. \end{aligned}$$

Eliminating α and β gives the condition $S_1^3 - 2S_1S_2 + S_3 = 0$. Now, we have

$$\begin{aligned} S_1(H_{a,b,c}^{-1}) &\equiv -q(a^a b^b c^c), && (3.8) \\ S_2(H_{a,b,c}^{-1}) &\equiv 0, && (3.9) \\ S_3(H_{a,b,c}^{-1}) &\equiv -\frac{B_{p-3}}{3}(a^3 + b^3 + c^3) \equiv -abcB_{p-3}. && (3.10) \end{aligned}$$

It is explained in [McC88], Lemma 5.24, how equation (3.8) follows from [Van20, 17]; equation (3.9) follows from parity considerations; and equation (3.10) follows from [Van20, 16], in exactly the same way as (3.8) follows from [Van20, 17]. □

We now define p-adic discs in Y, to which we apply Lemma 3.2. Let X be the sub-affinoid of Y defined by $|t| \leq 1$ in the wild case and by $|s| \leq |\pi_K|$ in the tame case. Let E_w be the quadratic unramified extension of K_w. If $F_{a,b,c}$ is wild, X is isomorphic to a union of two closed discs, which are defined over K_w in the split case and over E_w in the nonsplit case. Furthermore, $T = t$ is a parameter on each disc. If $F_{a,b,c}$ is tame, then X is isomorphic to a union of p closed discs defined over K_w, and $T = s/\pi_K$ is a parameter on each disk. For proofs of these facts we refer the reader to[McC88] (where $T = s'$ in the tame case). We denote by Z any of the discs that are components of X, with parameter T. We can write

$$f_i|_X = C_i u_i(T) v_i(T^p) g_i(T)^p, \quad i = 1, 2, 3, 4,$$

where u_i and v_i are unit power series with constant term 1 and integer coefficients, u_i has no terms in T^p, and g_i is a monic polynomial with integer coefficients. Furthermore, these conditions uniquely determine the u_i, v_i and g_i. Then

$$\frac{df_i}{f_i} \equiv \frac{du_i}{u_i} \pmod{_Z\ p}. \tag{3.11}$$

For a p-adic field H we denote by $U_H[[T]]$ the power series in $\mathcal{O}_H[[T]]$ which are congruent to 1 modulo the maximal ideal in $\mathcal{O}_H[[T]]$.

Theorem 3.6 *Let Z be any of the discs that are components of X and let T be a parameter on Z. Then*

$$u_i = 1 + \pi^{(p+3)/2-i} D_i T + O(\pi^{(p+5)/2-i} T), \tag{3.12}$$

where $|D_i| \leq 1$, $i = 1, 2, 3, 4$. Moreover, $|D_1| = 1$, and under the hypotheses of Theorem 1.4, $|D_4| = 1$ and

$$\frac{D_4}{D_1} \equiv q(a^a b^b c^c)^3 + abcB_{p-3}.$$

Finally, u_i for $i = 1, 2, 3$ are defined over E_w, and

$$u_4 \in 1 + \pi_K^{(p-5)/2} D_4 T U_{E_w}[[T]] + \pi_K^{(p+1)/2} \pi_L^{-3} E D_1 T U_{F_w}[[T]],$$

where $E \in \mathbb{Z}/p\mathbb{Z}^\times$ is independent of the triple (a, b, c) and F_w is the quadratic unramified extension of L_w.

Proof In both wild and tame cases we have $\omega_k \equiv \pi D\, dT \pmod{_Z\ \pi^2}$ for all $k \in H_{a,b,c}$, with $D \in \mathbb{Z}/p\mathbb{Z}^\times$ independent of k. This follows from our normalization (3.4), since in the tame case we have

$$s = \pi T, \tag{3.13}$$

and in the wild case it follows from [McC88, (5.6)], where it is shown that the expansion of s in terms of t on either of the discs in X is

$$s^2 = \frac{-q(a^a b^b c^c) 2b}{ac} + \pi \frac{2b}{ac}(t^p - t) + O(\pi^2). \tag{3.14}$$

The statements about D_1 follow from (3.2), (3.13) (in the tame case) and (3.14) (in the wild case), since $f_1 = x$. The statement about D_2 was proved in [McC88, Theorem 5.13]. Although this theorem is stated only for the wild split case, the consequence (3.12) is easily seen to hold also in the other cases (the part of Theorem 5.13 specific to the wild split case translates into the statement $|D_2| = 1$ in the current notation, and we do not need it here). The statements about D_3 and D_4 follow from Proposition 3.4, Lemma 3.5, and (3.11). The statement about the ratio D_4/D_1 follows from (3.5), the case $i = 0$ of (3.6), (3.7), and Lemma 3.5, taking note of the normalization (3.4) and the fact that $ds \equiv \text{unit} \times \pi dT \pmod{_Y \pi^2}$. The statements about the fields of definition follow from the fact that f_i is defined over K for $i = 1, 2, 3$ and f_4 is defined over L, and that the discs Z are always defined over E_w. The final statement follows from considerations of ramification theory. Locally, we have $\eta_{p-3} = 1 + a\pi^{p-3}$ modulo pth powers, so the (upper) conductor of L_w/K_w is 3. Now, it follows from the properties of the P_i that $u_4^{\sigma-1} \equiv u_1$ modulo $\mathcal{O}_{F_w}[[T]]^{\times p} U_{F_w}[[T^p]]$, and, since $u_1 \in 1 + \pi^{(p+1)/2} T D_1 U_{F_w}[[T]]$, this implies the final statement with E such that $(\sigma - 1)\pi_L^{-3} \equiv E^{-1} \pmod{\pi_L}$. $\square$

4 Computation of the Cassels pairing

Recall the local descent maps

$$\delta_i = \iota_{P_1} \times \cdots \times \iota_{P_i} \colon J(K_w) \to (K_w^\times / K_w^{\times p})^i$$

described in Section 2. We start by noting a couple of properties that follow from the choice of P_i made in Section 2. First, we have

$$\iota_{P_i} \circ \lambda = \iota_{P_{i-1}}, \quad i = 2, 3, 4. \tag{4.1}$$

Second, for $i = 1, 2, 3$ we have, from eigenspace considerations,

$$\iota_{P_i}(J(K_w)(k)) \subset V(k - i + 1). \tag{4.2}$$

Let $A \subset J(K_w)$ be the subgroup generated by divisors supported on the discs $|T| \le |\pi_K|$ in X. Let

$$V[i, j] = \bigoplus_{i \le k \le j} V(k).$$

Note that $V(i) = 0$ for $i > p$.

Proposition 4.1 *We have*

$$\iota_{P_i}(A) \subset V\big[(p + 5)/2 - i, p\big], \quad i = 1, 2, 3. \tag{4.3}$$

If $F_{a,b,c}$ is wild split, we have

$$\iota_{P_i}(J(K_w)) \subset V\big[(p+1)/2 - i, p\big], \quad i = 1, 2, 3. \tag{4.4}$$

If $F_{a,b,c}$ is wild nonsplit or tame, we have

$$\iota_{P_i}(J(K_w)) \subset V\big[(p+3)/2 - i, p\big], \quad i = 1, 2, 3. \tag{4.5}$$

Furthermore, in the case $i = 1$, the inclusions in (4.3) and (4.5) are equalities.

Proof The inclusions in (4.3) follow immediately from Theorem 3.6, as does the claim that the inclusion is equality in the case $i = 1$. Now Faddeev [Fad61] proved that

$$\operatorname{im} \iota_{P_1} = \begin{cases} V((p-1)/2) \oplus V[(p+3)/2, p] & \text{if } F_{a,b,c} \text{ is wild split,} \\ V[(p+1)/2, p] & \text{otherwise.} \end{cases}$$

This implies the statements (4.4) and (4.5) in the case $i = 1$, and also that the image of A in $J(K_w)/\lambda J(K_w)$ has codimension 1, and the eigenvalue of the quotient is $\kappa^{(p-1)/2}$ in the wild split case and $\kappa^{(p+1)/2}$ in the other cases. The remaining statements now follow from (4.1), (4.2), and (4.3). □

Proposition 4.2 *If $F_{a,b,c}$ is wild nonsplit or tame, then*

$$\delta_2(J(K_w)) = V\big[(p+1)/2, p\big]^2.$$

Proof From (4.1) with $i = 2$ we have

$$\operatorname{im} \delta_2 \cap (K^\times/K^{\times p}) \times 1 = \operatorname{im} \delta_1 \times 1 = V\big[(p+1)/2, p\big] \times 1 \tag{4.6}$$

Furthermore, given $u \in V[(p+3)/2, p]$, we can find $a \in A$ such that $\iota_{P_1}(a) = u$, and $\iota_{P_2}(a) \in V[(p+1)/2, p] \subset \operatorname{im} \iota_{P_1}$. Thus, modifying a by $\lambda J(K_w)$, we can choose it so that $\iota_{P_2}(a) = 1$. Hence

$$\operatorname{im} \delta_2 \supset 1 \times V\big[(p+3)/2, p\big]. \tag{4.7}$$

Now it follows from local duality that $\operatorname{im} \delta_2$ must be maximal isotropic with respect to the cup product pairing on $(K^\times/K^{\times p})^2 = H^1(K, J[\lambda^2])$ induced by the Weil pairing on $J[\lambda^2]$. Since $\lambda^2 = \hat{\lambda}^2$, the Weil pairing is skew symmetric. Thus the pairing on $(K^\times/K^{\times p})^2$ is a nonzero multiple of $((a_1, b_1), (a_2, b_2)) \mapsto (a_1, b_2)_w (b_1, a_2)_w^{-1}$, where $(\ ,\ )_w$ denotes the Hilbert symbol at w. The only maximal isotropic subgroup satisfying (4.6) and (4.7) is the one given in the statement of the proposition. □

Define a subspace $V_{\text{global}} \subset V$ by

$$V_{\text{global}} = \bigoplus_{\substack{2 \le i \le p-3 \\ i \text{ even}}} V(i).$$

Proposition 4.3 *Assume $p \geq 11$ and $F_{a,b,c}$ is wild nonsplit or tame. There exists a point $x \in A$ such that $\iota_{P_1}(x)$ generates $V((p+5)/2)$ and $\iota_{P_i}(x) \in V_{\text{global}}$ for $i = 2, 3$.*

Proof It follows from Proposition 4.1 that A, regarded as a $\mathbb{Z}_p[\zeta]$-submodule of $J(K_w)$, has codimension at most 1. Hence $\delta_3(A)$ has codimension ≤ 3 as a $\mathbb{F}_p$-vector space in $\delta_3(J(K_w))$. By Proposition 4.1 we can choose $x \in A$ such that $\iota_{P_1}(x)$ generates $V((p+5)/2)$. This condition leaves freedom to modify x by anything in $\lambda J(K_w)$, which would change $\delta_3(x)$ by anything in $\operatorname{im}\delta_2$. Thus, modifying x as needed, we can ensure that $\iota_{P_i}(x) \in V_{\text{global}}$, $i = 2, 3$. The number of degrees of freedom in performing this modification is equal to the dimension of $\operatorname{im}\delta_2 \cap V_{\text{global}}$, which is at least 4 if $p \geq 11$, by Proposition 4.2. Thus we can ensure that x remains in A when making the modification. □

Computation of the Cassels pairing for Theorem 1.2 We now use Proposition 2.1 to show that the pairing $\langle\ ,\ \rangle_2$ is trivial under the hypotheses of Theorem 1.2. In the next section we explain how this implies the theorem.

Denote by $\ell_i \colon S_{\lambda^i} \to J(K_w)/\lambda^i J(K_w)$ the localization map. We claim that, under the hypotheses of Theorem 1.2, $\iota_{P_1}(\ell_1(S_\lambda)) \subset V[(p+3)/2, p]$ or $\iota_{P_1}(\ell_1(S_\lambda)) \subset V((p+1)/2) \oplus V[(p+5)/2, p]$. Now, $V(i)$ pairs nontrivially with $V(j)$ under the Hilbert pairing if and only if $i + j \equiv p \pmod{p-1}$. Thus, it follows from our claim and from (4.2) that $\iota_{P_3}(\ell_3(J(K_w))$ pairs trivially with $\iota_{P_1}(\ell_1(J(K_w))$.

To see the claim, note that if hypothesis (a) of Theorem 1.2 is satisfied, namely that $F_{a,b,c}$ is wild split and $p \equiv 3 \pmod 4$, then, by [Fad61], $\iota_{P_1}(\ell_1(S_\lambda)) \subset V((p-1)/2) \oplus V[(p+3)/2, p]$. Furthermore, we can eliminate $V((p-1)/2)$ as a possibility, because ℓ_1 factors through $H^1(K(p)/K, \mu_p) \to H^1(K_w, \mu_p)$. Since $(p-1)/2$ is odd, it follows from (2.4) that ℓ_1 can have nontrivial image in $V((p-1)/2)$ only if $C((p-1)/2)$ is nontrivial, which would imply $p \mid B_{(p+1)/2}$. This never happens if $p \equiv 3 \pmod 4$.

If hypothesis (b) of Theorem 1.2 is satisfied, namely that $F_{a,b,c}$ is wild nonsplit or tame and the image of U in either $V((p+1)/2)$ or $V((p+3)/2)$ is trivial, then the claim follows immediately from (4.5).

The proof of Theorem 1.4 uses the following lemma.

Lemma 4.4 *Suppose $p \geq 5$ is regular, and let L be as in (2.2). Then*

1. *the map $H^1(K(p)/L, \mu_p) \to H^1(L_w, \mu_p)$ is injective*
2. *the norm map $N_{L/K} \colon \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective*
3. *$H^1(K(p)/L, \mu_p)^G(i) = 0$ if i is odd and $i \neq 1$, or if $i = p - 1$.*

Proof Let H_K (resp. H_L) be the Hilbert class field of K (resp. L). Since L/K is unramified outside p, and there is only prime of L above p, it follows that $\mathrm{Gal}(H_L/L)/(\sigma - 1) \simeq \mathrm{Gal}(H_K/K)$. Therefore p does not divide the order of the class group $C_L \simeq \mathrm{Gal}(H_L/L)$. The injectivity statement follows, since anything in the kernel would generate an unramified Kummer extension of L of degree p. Furthermore, every unit of K is a local norm everywhere except possibly at the prime above p, and therefore is a local norm there also by the product formula. Thus it is a global norm. The surjectivity of the norm map follows by a standard argument using $\mathrm{Gal}(L/K)$ cohomology of the sequences

$$1 \to \mathcal{O}_L^\times \to L^\times \to P_L \to 1 \quad \text{and} \quad 1 \to P_L \to I_L \to C_L \to 1,$$

where I_L and P_L are the groups of ideals and principal ideals respectively. Finally, by (2.4),

$$H^1(K(p)/K, \mu_p) = \mathcal{O}_K'^\times/\mathcal{O}_K'^{\times p} \quad \text{and} \quad H^1(K(p)/L, \mu_p) = \mathcal{O}_L'^\times/\mathcal{O}_L'^{\times p}.$$

Moreover, the cokernel of $\mathcal{O}_K^\times/\mathcal{O}_K^{\times p}$ in $(\mathcal{O}_L^\times/\mathcal{O}_L^{\times p})^G$ is $H^2(L/K, \mu_p) \simeq \mathbb{Z}/p\mathbb{Z}$, with $\mathrm{Gal}(K/\mathbb{Q})$ acting via κ^{p-3}, since it acts on G via κ^3. Since $p-3$ is even and $(\mathcal{O}_K^\times/\mathcal{O}_K^{\times p})(i) = 0$ if i is odd and $i \neq 1$, or if $i = p-1$, the third statement of the lemma follows. $\square$

Proof of Theorem 1.4 We exhibit $a \in S_{\lambda^3}$ and $b \in S_\lambda$ which pair non-trivially under the Cassels pairing.

Since p is regular, the exact sequence [McC88, 7.3] identifies U with $\mathcal{O}_K^\times/\mathcal{O}_K^{\times p}$. Thus $S_{\lambda^i} \subset (\mathcal{O}_K^\times/\mathcal{O}_K^{\times p})^i$ for $i \leq 3$. The Selmer group is the subgroup obtained by imposing the local conditions at w. Since $(p+1)/2$ is even, we can choose an element $b \in \mathcal{O}_K^\times/\mathcal{O}_K^{\times p}$ which generates $V((p+1)/2)$, and b satisfies the local condition by Proposition 4.1, so $b \in S_\lambda$.

As for a, by Proposition 4.3 there exists $a_w = (a_{w,1}, a_{w,2}, a_{w,3}) = \delta_3(x)$, $x \in A$, such that $a_{w,1}$ generates $V((p+5)/2)$ and $a_{w,2}, a_{w,3} \in V_{\mathrm{global}}$. Using a suitable projector, we may further assume that x is an eigenvector for the action of Δ. Choose eigenvectors $a_i \in \mathcal{O}_K^\times/\mathcal{O}_K^{\times p}$ specializing to $a_{w,i}$ for $i = 1, 2, 3$ and define $a \in S_{\lambda^3}$ by $a = (a_1, a_2, a_3)$.

Now, by Lemma 4.4, $\lambda_*^2 a = a_1 \in V((p+5)/2)$ is the norm of a global unit ϵ in $\mathcal{O}_L^\times$, and by Proposition 2.3, the Cassels pairing of a and b is the Hilbert pairing (c_w, b_w), where $c_w \in K^\times/K^{\times p}$ is an eigenvector and

$$c_w = \iota_{P_4}(x)^{-1} \eta N' \epsilon \quad \text{in } L_w^\times/L_w^{\times p}, \tag{4.8}$$

where $\eta \in H^1(K(p)/L, \mu_p)^G$. We can identify the precise eigenspace in which c_w lies as follows. Since $a_{w,1} = \iota_{P_1}(x)$, and since P_1 is fixed by Δ, x has eigenvalue $\kappa^{(p+5)/2}$. Then, since λ has eigenvalue κ (modulo λ^5), it follows that $\delta_3(x)$, and hence c_w, have eigenvalue $\kappa^{(p+5)/2-3} = \kappa^{(p-1)/2}$. Thus we may assume without loss of generality that c_w, η, $N'\epsilon$, and $\iota_{P_4}(x)$ are eigenvectors for a lift $\tilde{\Delta}$ of $\Delta = \mathrm{Gal}(K_w/\mathbb{Q}_p)$ to $\mathrm{Gal}(L_w/\mathbb{Q}_p)$, with eigenvalue $\kappa^{(p-1)/2}$. Since $\eta \in H^1(K(p)/L, \mu_p)^G$, its projection onto an eigenspace $(L_w^\times/L_w^{\times p})(i)$ with $i > 1$ odd is trivial, by Lemma 4.4. This applies in particular to $i = (p-1)/2$, so that the image of η in $L_w^\times/L_w^{\times p}$ is trivial.

Under the Hilbert pairing the $\kappa^{(p-1)/2}$ and $\kappa^{(p+1)/2}$ eigenspaces of $K_w^\times/K_w^{\times p}$ pair nontrivially. Thus, to prove that the pairing (c_w, b_w) is nontrivial, it suffices to show that c_w is not a pth power, and for that it suffices to show that its image in $L_w^\times/L_w^{\times p}$ is nontrivial.

Since $x \in A$, we may choose a divisor D supported on $|T| \leq |\pi|$ such that $a_{w,i} = f_i(D)$, $1 \leq i \leq 3$. Since D is supported on $|T| \leq |\pi|$, we have

$$u = f_4(D) \equiv u_4(D) \pmod{L_w^{\times p}(1 + \pi^p \mathcal{O}_{L_w})}.$$

From the Galois properties of the P_i, we have

$$u \in (L_w^\times/L_w^{\times p})((p-1)/2)), \quad (\sigma - 1)u = v, \tag{4.9}$$

where v is the image in $L_w^\times/L_w^{\times p}$ of a generator of $V((p+5)/2)$. Since $p \geq 19$, $(p+5)/2$ is less than $p-3$, and thus $v \neq 0$. Thus the subspace of $L_w^\times/L_w^{\times p}$ satisfying the conditions (4.9) is two-dimensional, with generators u_1 and u_2, where u_1 is the image of a generator of $V((p-1)/2)$ with expansion $u_1 = 1 + \pi_K^{(p-1)/2} + O(\pi_K^{(p+1)/2})$, and $u_2 \in (L_w^\times/L_w^{\times p})((p-1)/2)$ has expansion $u_2 = 1 + \pi_K^{(p+5)/2}\pi_L^{-3} + O(\pi_K^{(p+5)/2})$. Thus $u = u_1^\alpha u_2^\beta$ for some $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$. Expanding the binomial series, we get

$$u = 1 + \alpha\pi_K^{(p-1)/2} + \beta\pi_K^{(p+5)/2}\pi_L^{-3} + O(\pi_K^{p-1}). \tag{4.10}$$

We can now use Theorem 3.6 to evaluate u_4 at D. Comparing appropriate coefficients (note that D is supported on $|T| \leq |\pi|$), we see that

$$\frac{\alpha}{\beta} = \frac{D_4}{ED_1} = \frac{1}{E}\gamma(a,b,c) = \frac{1}{E}(q(a^a b^b c^c)^3 + abcB_{p-3}). \tag{4.11}$$

Now, we may replace (a,b,c) by any $(a',b',c') \equiv (ta,tb,tc) \pmod p$, for $t \in \mathbb{F}_p^\times$. It is easily seen, using the property $q(xy) \equiv q(x) + q(y)$, that $\gamma(ta,tb,tc) \equiv t^3\gamma(a,b,c)$. Thus, from (4.11), we see that by varying t appropriately we may ensure that u, and hence c_w, varies in $L_w^\times/L_w^{\times p}$, and, in particular, takes on nonzero values. Hence there exists a choice of t such that the pairing is nontrivial for the curve $F_{a',b',c'}$. However, this curve is isomorphic to $F_{a,b,c}$, and hence the pairing must be nontrivial in that case as well. $\square$

5 Shafarevich–Tate groups

The proofs of Theorem 1.2 and Theorem 1.5 follow from the computations of the Cassels–Tate pairing by means of the following proposition.

Proposition 5.1 *For all positive integers m and n, the restriction of the Cassels–Tate pairing induces a perfect pairing*

$$\Big(Ш[\lambda^m]/(\lambda^n Ш[\lambda^{n+m}])\Big) \times \Big(Ш[\lambda^n]/(\lambda^m Ш[\lambda^{n+m}])\Big) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Let $Ш_{\mathrm{div}}$ denote the maximal divisible subgroup of $Ш$, i.e. $x \in Ш_{\mathrm{div}}$ if and only if for every nonzero integer n there exists $y \in Ш$ such that $x = ny$. Let $Ш_{\mathrm{red}}$ denote the quotient group $Ш/Ш_{\mathrm{div}}$. Note that:

Lemma 5.2 *$Ш_{\mathrm{div}}$ is a divisible group in the usual sense that multiplication by any nonzero $n \in \mathbb{Z}$ is surjective on it.*

Proof The argument is standard: since $Ш[m]$ is finite for all nonzero $m \in \mathbb{Z}$, the groups $NШ[Nm]$, $N > 0$, stabilize for sufficiently large N. Thus for every m there is an integer $N(m)$ such that if an element of $Ш[m]$ is divisible by $N(m)$ it is infinitely divisible. Now if $x \in Ш_{\mathrm{div}}[m]$ and $n > 0$, choose $y \in Ш[N(nm)nm]$ such that $N(nm)ny = x$. Then $y' = N(nm)y$ is in $Ш_{\mathrm{div}}[nm]$ and $ny' = x$. □

Note that since ζ is an automorphism of $Ш$ it preserves $Ш_{\mathrm{div}}$, and hence so does $\mathbb{Z}[\zeta]$. Furthermore, since λ^{p-1} is a unit times p in $\mathbb{Z}[\zeta]$, $Ш_{\mathrm{div}}$ is divisible by λ^n for any positive n.

Lemma 5.3 *The exact sequence*

$$0 \longrightarrow Ш_{\mathrm{div}} \longrightarrow Ш \longrightarrow Ш_{\mathrm{red}} \longrightarrow 0$$

induces by restriction an exact sequence

$$0 \longrightarrow Ш_{\mathrm{div}}[\lambda^n] \longrightarrow Ш[\lambda^n] \longrightarrow Ш_{\mathrm{red}}[\lambda^n] \longrightarrow 0$$

for any positive integer n.

Proof Only the surjectivity is in question. Let $x \in Ш_{\mathrm{red}}[\lambda^n]$. Lift x to $y \in Ш$. Then $\lambda^n y = z \in Ш_{\mathrm{div}}$. By Lemma 5.2, we can find $w \in Ш_{\mathrm{div}}$ such that $\lambda^n w = z = \lambda^n y$. But then $y - w \in Ш[\lambda^n]$ and $y - w$ reduces to x in $Ш_{\mathrm{red}}$. □

It is well known that $Ш_{\mathrm{red}}[p^\infty]$ is a finite group and that the Cassels–Tate pairing induces a perfect pairing

$$[\cdot\,\cdot]\colon Ш_{\mathrm{red}}[p^\infty] \times Ш_{\mathrm{red}}[p^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

We now have the following lemma:

Lemma 5.4 *The annihilator of* $Ш_{\mathrm{red}}[\lambda^m]$ *with respect to the latter pairing equals* $\lambda^m Ш_{\mathrm{red}}[p^\infty]$*, for all positive integers* m*.*

Proof It is clear from the definition of the pairing given in [McC88], for example, and from the functoriality properties of the Weil pairing, that $[\zeta a, a'] = [a, \zeta^{-1}a']$. Hence, if $\hat{\lambda} = \zeta^{-1} - 1$, then $\hat{\lambda}^m Ш_{\mathrm{red}}[p^\infty]$ annihilates $Ш_{\mathrm{red}}[\lambda^m]$. Since $\hat{\lambda}/\lambda$ is a unit in $\mathbb{Z}[\zeta]$, we have $\hat{\lambda}^m Ш_{\mathrm{red}}[p^\infty] = \lambda^m Ш_{\mathrm{red}}[p^\infty]$. So the kernel H on the right factor of the restricted pairing

$$Ш_{\mathrm{red}}[\lambda^m] \times Ш_{\mathrm{red}}[p^\infty] \longrightarrow \mathbb{Q}/\mathbb{Z}$$

contains $\lambda^m Ш_{\mathrm{red}}[p^\infty]$. Note that the kernel on the left factor of the latter pairing is trivial. Therefore, the cardinalities of $Ш_{\mathrm{red}}[\lambda^m]$ and $Ш_{\mathrm{red}}[p^\infty]/H$ are equal. But

$$|Ш_{\mathrm{red}}[p^\infty]| = |Ш_{\mathrm{red}}[\lambda^m]|\ |\lambda^m Ш_{\mathrm{red}}[p^\infty]|,$$

hence $H = \lambda^m Ш_{\mathrm{red}}[p^\infty]$. $\square$

Lemma 5.5 *For all positive integers* m *and* n*, the restriction of the Cassels–Tate pairing induces a perfect pairing*

$$\Big(Ш_{\mathrm{red}}[\lambda^m]/(\lambda^n Ш_{\mathrm{red}}[\lambda^{n+m}])\Big) \times \Big(Ш_{\mathrm{red}}[\lambda^n]/(\lambda^m Ш_{\mathrm{red}}[\lambda^{n+m}])\Big) \longrightarrow \mathbb{Q}/\mathbb{Z}.$$

Proof By Lemma 5.4, the annihilator of $Ш_{\mathrm{red}}[\lambda^m]$ in $Ш_{\mathrm{red}}[\lambda^n]$ equals

$$\lambda^m Ш_{\mathrm{red}}[p^\infty] \cap Ш_{\mathrm{red}}[\lambda^n] = \lambda^m Ш_{\mathrm{red}}[\lambda^{n+m}],$$

and the assertion follows. $\square$

Proof of Proposition 5.1 By Lemma 5.5, it suffices to show that for all m and n the groups $Ш[\lambda^m]/(\lambda^n Ш[\lambda^{n+m}])$ and $Ш_{\mathrm{red}}[\lambda^m]/(\lambda^n Ш_{\mathrm{red}}[\lambda^{n+m}])$ are isomorphic. By Lemma 5.3, we have a commutative diagram

$$\begin{array}{ccccccccc}
0 & \to & Ш_{\mathrm{div}}[\lambda^{n+m}] & \longrightarrow & Ш[\lambda^{n+m}] & \longrightarrow & Ш_{\mathrm{red}}[\lambda^{n+m}] & \to & 0 \\
 & & \big\downarrow \alpha = \lambda^n & & \big\downarrow \beta = \lambda^n & & \big\downarrow \gamma = \lambda^n & & \\
0 & \to & Ш_{\mathrm{div}}[\lambda^m] & \longrightarrow & Ш[\lambda^m] & \longrightarrow & Ш_{\mathrm{red}}[\lambda^m] & \to & 0
\end{array}$$

where the horizontal sequences are exact. By the Snake Lemma, we get an exact sequence

$$\begin{aligned} 0 \to \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\beta) \to \mathrm{Ker}(\gamma) \to \\ \to \mathrm{Coker}(\alpha) \to \mathrm{Coker}(\beta) \to \mathrm{Coker}(\gamma) \to 0. \end{aligned}$$

By Lemma 5.2, we have $\mathrm{Coker}(\alpha) = 0$, hence $\mathrm{Coker}(\gamma)$ is isomorphic to $\mathrm{Coker}(\beta)$, and this completes the proof. $\square$

Proof of Theorem 1.2 By the structure theorem for torsion modules over Dedekind domains we have a $\mathbb{Z}[\zeta]$-module decomposition

$$Ш[\lambda^3] \simeq (\mathbb{Z}[\zeta]/(\lambda))^{t_1} \oplus (\mathbb{Z}[\zeta]/(\lambda^2))^{t_2} \oplus (\mathbb{Z}[\zeta]/(\lambda^3))^{t_3},$$

where t_1, t_2 and t_3 are nonnegative integers. The computations in the previous section show that the pairing (obtained by restricting the Cassels–Tate pairing)

$$Ш[\lambda^2] \times Ш[\lambda] \to \mathbb{Q}/\mathbb{Z}$$

is trivial. By Proposition 5.1 (for $m = 2$ and $n = 1$), we get that the groups $Ш[\lambda^2]/(\lambda Ш[\lambda^3])$ and $Ш[\lambda]/(\lambda^2 Ш[\lambda^3])$ are both trivial. But then

$$(\mathbb{Z}[\zeta]/(\lambda))^{t_1} \oplus (\mathbb{Z}[\zeta]/(\lambda))^{t_2} \oplus (\mathbb{Z}[\zeta]/(\lambda))^{t_3} \simeq Ш[\lambda] = \lambda^2 Ш[\lambda^3] \simeq (\mathbb{Z}[\zeta]/\lambda)^{t_3}$$

so $t_1 = t_2 = 0$, which proves the claim. □

Proof of Theorem 1.5 Let

$$Ш[\lambda^4] \simeq (\mathbb{Z}[\zeta]/(\lambda))^{a} \oplus (\mathbb{Z}[\zeta]/(\lambda^2))^{b} \oplus (\mathbb{Z}[\zeta]/(\lambda^3))^{c} \oplus (\mathbb{Z}[\zeta]/(\lambda^4))^{d}.$$

If we show that $d = 0$, then λ^3 annihilates $Ш[\lambda^4]$, therefore $Ш[\lambda^4] = Ш[\lambda^3]$. By induction, this implies $Ш[p^\infty] = Ш[\lambda^\infty] = Ш[\lambda^3]$. So assume $d \geq 1$. Since the Cassels–Tate pairing on $Ш[\lambda^3] \times Ш[\lambda]$ is nontrivial, Proposition 5.1 implies that $Ш[\lambda^3]/(\lambda Ш[\lambda^4])$ has dimension ≥ 2 over $\mathbb{F}_p$. Now

$$\lambda Ш[\lambda^4] \simeq (\mathbb{Z}[\zeta]/(\lambda))^{b} \oplus (\mathbb{Z}[\zeta]/(\lambda^2))^{c} \oplus (\mathbb{Z}[\zeta]/(\lambda^3))^{d}.$$

Counting $\mathbb{F}_p$-dimensions, we get $6-(b+2c+3d) \geq 2$, therefore $b+2c+3d \leq 4$. This implies $d = 1$ and $c = 0$. Therefore,

$$Ш[\lambda^4] \simeq (\mathbb{Z}[\zeta]/(\lambda))^{a} \oplus (\mathbb{Z}[\zeta]/(\lambda^2))^{b} \oplus (\mathbb{Z}[\zeta]/(\lambda^4)).$$

This implies that

$$(\mathbb{Z}[\zeta]/(\lambda))^2 = \lambda^2(\mathbb{Z}[\zeta]/(\lambda^3))^2 \simeq \lambda^2 Ш[\lambda^3] \subseteq \lambda^2 Ш[\lambda^4] \simeq \mathbb{Z}[\zeta]/(\lambda^2),$$

a contradiction. □

6 Tame reduction

Although it is not strictly necessary for Theorem 1.6, we take the opportunity to prove a general lemma on tame reduction, since it clears up some confusion in the literature. In [Lim95], an attempt was made to improve the result of

[McC88] on the existence of nontrivial elements in Ш$[\lambda]$ in the wild split case, under the additional hypothesis that the Jacobian of the Fermat curve in question is nonsimple. However, as Lemma 6.1 shows, nonsimple Jacobian and wild split reduction over $\mathbb{Z}_p[\zeta]$ are incompatible properties, so the Mordell–Weil rank estimates given in the last section of [Lim95] are incorrect. As far as we can tell, the problem lies in the use of the function $q(x)$ which computes the reduction type (see the introduction). Here as well as in [McC88], q is evaluated on triples (a, b, c) of integers such that $0 < a, b, a+b < p$ and $a+b+c = 0$. In [Lim95] however, q is evaluated on triples (a, b, c) such that $0 < a, b, a+b < p$ and $a+b+c = p$. While it does not make any difference which of the two types of triples one chooses to define the curve $F_{a,b,c}$, it does make a difference which type of triple one uses to evaluate q and hence the reduction type. We have the following lemma:

Lemma 6.1 *Let (a, b, c) be such that $J_{a,b,c}$ is nonsimple. Then $F_{a,b,c}$ has tame reduction over $\mathbb{Z}_p[\zeta]$.*

Proof By [KR78], $J_{a,b,c}$ is nonsimple if and only if $p \equiv 1 \pmod 3$ and $F_{a,b,c}$ is isomorphic to $F_{1,r,-(r+1)}$, where $r^2+r+1 = 0$ in $\mathbb{F}_p$. By definition of $q(x)$, it therefore suffices to show that $(r+1)^{(r+1)(p-1)} - r^{r(p-1)} \equiv 0 \pmod{p^2}$. Since 6 divides $p-1$, it suffices to show that

$$(r+1)^{6(r+1)} - r^{6r} \equiv 0 \pmod{p^2}.$$

Let k be an integer such that $r^2 + r + 1 = pk$. Then $(r+1)^2 = pk + r$. Therefore,

$$(r+1)^6 = (pk+r)^3 \equiv r^3 + 3r^2pk \pmod{p^2}.$$

Hence $(r+1)^{6(r+1)} \equiv (r^3 + 3r^2pk)^{r+1} \equiv (r^{3(r+1)} + 3r^2pk(r+1)r^{3r}) \pmod{p^2}$. Now note that $r^{3r}r^2(r+1) \equiv -r \pmod p$ since r is a cube root of unity modulo p, so that $3r^2pk(r+1)r^{3r} \equiv -3rpk \pmod{p^2}$. Hence, $(r+1)^{6(r+1)} \equiv (r^{3r+3} - 3rpk) \pmod{p^2}$. Therefore,

$$(r+1)^{6(r+1)} - r^{6r} \equiv (r^{3r}(r^3 - r^{3r}) - 3rpk) \pmod{p^2}.$$

Since $r^3 = pk(r-1)+1$, we get $r^{3r} \equiv (rpk(r-1)+1) \pmod{p^2}$, so $r^3 - r^{3r} \equiv -pk(r-1)^2 \pmod{p^2}$. Hence,

$$(r+1)^{6(r+1)} - r^{6r} \equiv -pk(r^{3r}(r-1)^2 + 3r) \pmod{p^2}.$$

Since $r^{3r}(r-1)^2 + 3r \equiv 0 \pmod p$, this proves the proposition. □

Remark A less computational proof of Lemma 6.1 was suggested to us by Dino Lorenzini. The argument goes as follows: To show that the reduction is tame, it suffices, by work of McCallum, to show that the degree of the minimum extension M/K_w^{unr} such that $J_{a,b,c}$ has good reduction over M is prime to p. It is known that this minimum degree is at most $2g+1$. Now suppose $J_{a,b,c}$ is isogenous to the product of two abelian varieties of smaller dimension. Then M is the compositum of the corresponding minimum extensions for the factors. Each of the latter extensions has degree strictly less than p, so the degree of their compositum is prime to p.

Proof of Theorem 1.6 By Lemma 6.1, the reduction is tame in this case. By Theorem 1.4 and Proposition 5.1, the $\mathbb{F}_p$-dimension of $Ш[\lambda]/(\lambda^3 Ш[\lambda^4])$ is ≥ 2. In particular, the $\mathbb{F}_p$-dimension of $Ш[\lambda]$ is ≥ 2. Since p is regular, the results of Faddeev ([Fad61]) show that the Selmer group S_λ is 3-dimensional over $\mathbb{F}_p$. On the other hand, Gross and Rohrlich ([GR78]) have shown that the Mordell–Weil rank of $J_{7,1,-8}$ over $\mathbb{Q}$ is nonzero. Therefore, the rank equals 1 and $Ш[\lambda]$ is 2-dimensional over $\mathbb{F}_p$. By Theorem 1.2 it follows that $Ш[\lambda^3]$ has rank 2 over $\mathbb{Z}[\zeta]/(\lambda^3)$. Theorem 1.5 then implies that $Ш[p^\infty] \simeq (\mathbb{Z}[\zeta]/(\lambda^3))^2$. The statement about quadratic points on $F_{7,1,-8}$ and on the Fermat curve $X^{19}+Y^{19}+Z^{19}=0$ follows immediately from Corollary 2.2 and Theorem 1.3 of [Tze02]. $\square$

References

[BGR84] Siegfried Bosch, Ulrich Güntzer and Reinhold Remmert, *Non-Archimedean analysis*, A systematic approach to rigid analytic geometry, Springer, 1984

[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** (1981) 345–359

[KR78] Neal Koblitz and David Rohrlich, *Simple factors in the Jacobian of a Fermat curve*, Canad. J. Math. **30** (1978) 1183–1205

[Kur92] Masato Kurihara, *Some remarks on conjectures about cyclotomic fields and k-groups of $\mathbb{Z}$*, Compositio Math. **81** (1992) 223–226

[Lim95] Chong-Hai Lim, *The Shafarevich–Tate group and the Jacobian of a cyclic quotient of a Fermat curve*, Arch. Math. (Basel) **64** (1995) 17–21

[McC82] William G. McCallum, *The degenerate fiber of the Fermat curve*, Number theory related to Fermat's last theorem (Cambridge, Mass., 1981) (N. Koblitz, ed.), Progress in Mathematics, Birkhaüser, 1982, pp. 57–70

[McC88] William G. McCallum, *On the Shafarevich–Tate group of the Jacobian of a quotient of the Fermat curve*, Invent. Math. **93** (1988) 637–666

[NSW00] Jürgen Neukirch, Alexander Schmidt and Kay Wingberg, *Cohomology of Number Fields*, Springer-Verlag, Berlin, 2000

[Tze02] Pavlos Tzermias, *Low-degree points on Hurwitz–Klein curves*, Recommended for publication in Trans. Amer. Math. Soc. 2002

[Van20] Hugh S. Vandiver, *A property of cyclotomic integers and its relation to Fermat's last theorem*, Ann. of Math. **21** (1919–1920) 73–80

William G. McCallum,
Department of Mathematics,
P.O. Box 210089, 617 N. Santa Rita,
The University of Arizona,
Tucson, AZ 85721-0089, USA
e-mail: wmc@math.arizona.edu

Pavlos Tzermias,
Department of Mathematics,
University of Tennessee,
Knoxville, TN 37996-1300, USA
e-mail: tzermias@math.utk.edu