BULL. AUSTRAL. MATH. SOC. 11D41, 11G30, 14G05, 14G25
VOL. 63 (2001) [393–406]

BRAUER POINTS ON FERMAT CURVES

WILLIAM G. MCCALLUM

In honour of George Szekeres on his 90th birthday

If X is a variety over a number field K, the set of K-rational points on X is contained in the subset of the adelic points cut out by the Brauer group; we call this set the set of Brauer points on the variety. If S is a set of valuations of K, we also define S-Brauer points in a natural way. It is natural to ask how good a bound on the rational points is provided by the Brauer (or S-Brauer) points.

Let $p > 3$ be a prime number, and let X be the Fermat curve of degree p, $x^p + y^p = 1$. Let K be the field of p-th roots of unity, and let r be the p-rank of the class group of K. In this paper we show that if $r < (p+3)/8$, then the set of p-Brauer points on X has cardinality at most p. We construct elements of the Brauer group of X by relating it to the Weil-Chatelet group of the jacobian of X, then use the method of Coleman and Chabauty to bound the points cut out by these elements.

1. INTRODUCTION

The Hasse principle is said to hold for a class of varieties over a number field K if for any variety X in the class, the set of rational points $X(K)$ is non-empty whenever the set of adelic points $X(\mathbb{A}_K)$ is non-empty. Manin [8] observed that the failure of the Hasse principle can often be explained in terms of the Brauer group of X, $\mathrm{Br}(X)$. The product rule implies that $X(K)$ must be contained in the set of *Brauer points*

$$X(\mathbb{A}_K)^{\mathrm{Br}} = \left\{ x \in X(\mathbb{A}_K) : \sum_v \mathrm{inv}_v\, a(x_v) = 0 \ \text{ for all } a \in \mathrm{Br}(X) \right\}$$

Received 6th December, 2000
This research was supported in part by National Science Foundation grants 9302976 and 9624219, and by an AMS Centennial Fellowship.
This paper comes out of work conducted during 1991–96, in part while visiting the Centre for Number Theory Research at Macquarie University, the Institut des Hautes Études Scientifiques, the Université de Bordeaux, and the Institute for Advanced Study; I would like to thank them for their hospitality. My renewed interest in it, and the formulation in terms of the Brauer group, were sparked by the talks on the Hasse principle at the Arizona Winter School in 1999 (Colliot-Thélène, Harari, Scharaschkin, and Skorobogatov). Finally, I would like to thank Greg Anderson, Robert Coleman, Jean-Louis Colliot-Thélène, Barry Mazur, and Bjorn Poonen for useful comments and criticisms.

where the sum is over a complete set of inequivalent valuations of K and inv_v is the canonical map $\mathrm{Br}(K_v) \simeq \mathbb{Q}/\mathbb{Z}$. The set of Brauer points is closed in the adelic topology, and therefore contains the closure $\overline{X(K)}$ of the rational points. Manin considered examples where elements in the Brauer group could be constructed that forced the set of Brauer points to be empty (and hence also the set of rational points), even though the set of adelic points was not. Thus the Hasse principle was violated.

If $X(K)$ is not empty, it is natural to wonder how good a bound on $\overline{X(K)}$ is $X(\mathbb{A}_K)^{\mathrm{Br}}$. For example, the following theorem is an immediate consequence of theorems of Scharaschkin [**13**, Theorems 1.1 and 1.2].

THEOREM. (Scharaschkin) *Let X be a smooth curve of positive genus with a K-rational point. Let J be the jacobian of X and suppose that the Mordell-Weil group and the Shafarevich-Tate group of J over K are finite. Then $X(K) = X(\mathbb{A}_K)^{\mathrm{Br}}$.*

In considering the question of Brauer points, it is convenient to focus on a restricted set of valuations. Suppose that X is proper, let $\mathcal{X}$ be a model for X proper over $\mathcal{O}_K$, and let S be a set of inequivalent valuations of K. For a valuation v, let K_v be the completion of K at v. If v is non-archimedean, let $\mathcal{O}_v$ be the ring of integers in K_v, and $j_v : X \times_K K_v \hookrightarrow \mathcal{X}_v = \mathcal{X} \times_{\mathcal{O}_K} \mathcal{O}_v$ the natural map. If v is archimedean, we adopt the convention that $\mathrm{Br}(\mathcal{X}_v) = 0$. For $a \in \mathrm{Br}(X)$, let a_v be the image of a under $\mathrm{Br}(X) \to \mathrm{Br}(X \times_K K_v)$. Define

$$\mathrm{Br}_S(\mathcal{X}) = \{a \in \mathrm{Br}(X) : a_v \in j_v^* \mathrm{Br}(\mathcal{X}_v),\ v \notin S\}.$$

Note that if $v \notin S$, then given $x_v \in X(K_v)$ and $a \in \mathrm{Br}_S(\mathcal{X})$ we have $a(x_v) = 0$. This is clear if v is archimedean, and if v is non-archimedean then by definition there is an element $\widetilde{a}_v \in \mathrm{Br}(\mathcal{X}_v)$ such that $a_v = j^*(\widetilde{a}_v)$, and since $\mathcal{X}$ is proper, there is a section $\widetilde{x}_v$ of $\mathcal{X}_v$ extending x_v, so $a(x_v) = a_v(x_v) = \widetilde{a}_v(\widetilde{x}_v) \in \mathrm{Br}(\mathcal{O}_v) = 0$. It makes sense to define the set of *S-Brauer points with respect to $\mathcal{X}$*

$$X(\mathbb{A}_{K,S})^{\mathrm{Br}_S(\mathcal{X})} = \left\{x \in X(\mathbb{A}_{K,S}) : \sum_{v \in S} \mathrm{inv}_v\, a(x_v) = 0 \ \text{ for all } \ a \in \mathrm{Br}_S(X)\right\},$$

where $\mathbb{A}_{K,S} = \Pi'_{v \in S} K_v$. The projection of $X(\mathbb{A}_K)^{\mathrm{Br}}$ onto its S-component is contained in the set of S-Brauer points and hence so is $X(K)$.

If $H \subset \mathrm{Br}_S$, we define $X(\mathbb{A}_{K,S})^H$ similarly, and refer to it as the S-Brauer points cut out by H; if $H = \langle a \rangle$, we talk about the S-Brauer points cut out by a.

Our question is now: how good a bound on $\overline{X(K)}$ is $X(\mathbb{A}_{K,S})^{\mathrm{Br}_S}$ for different choices of S?

Let p be an odd prime, and let F be the p^{th} Fermat curve over $\mathbb{Q}$, with projective equation

$$X^p + Y^p = Z^p. \tag{1}$$

https://doi.org/10.1017/S0004972700019493 Published online by Cambridge University Press

Then F has a proper model $\mathcal{F}$ over $\mathbb{Z}$ which has good reduction outside p. Let C be the ideal class group of the ring of integers in the field $\mathbb{Q}(e^{2\pi i/p})$. Let v_p be the p-adic valuation of $\mathbb{Q}$.

THEOREM A. *Suppose* $\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(C/pC) < (p+3)/8$. *Let* $S = \{v_p\}$ *(so that* $\mathbb{A}_{\mathbb{Q},S} = \mathbb{Q}_p$*). Then*

$$\left|F(\mathbb{Q}_p)^{\mathrm{Br}_S(\mathcal{F})}\right| \leqslant p.$$

It seems quite likely that the hypothesis is always satisfied: For $p \leqslant 12{,}000{,}000$, the largest value of the rank is 7 [3]. If Vandiver's conjecture is true then the rank is equal to the index of irregularity, whose expected value is, heuristically, $O(\log p/\log\log p)$ (see [14], Exercise 6.6). However, the best proven bound on the rank is $\operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(C/pC) < p/2$, which follows from a Carlitz's bound on the *size* of the minus part of the ideal class group [4, (21)] using the fact that the p-rank of the plus part is less than the p-rank of the minus part [14, Theorem 10.11].

The proof of Theorem A makes use of certain quotient curves. Let $\mu_p \subset \mathbb{C}$ be the group of p-th roots of unity, and let G be the quotient of μ_p^3 by the diagonally embedded μ_p. Then G acts as a group of automorphisms on F, via

$$(X,Y,Z) \mapsto (\zeta_1 X, \zeta_2 Y, \zeta_3 Z), \qquad (\zeta_1,\zeta_2,\zeta_3) \in \mu_p^3.$$

Let $\Gamma \subset G$ be a subgroup of order p, and let $F_\Gamma = F/\Gamma$. Since $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$, there are $p+1$ choices for Γ, hence we obtain $p+1$ quotient curves F_Γ. Three of them have genus 0, the other $p-2$ have genus $(p-1)/2$. We call these latter $p-2$ curves the *quotient Fermat curves*. If a, b, and c are integers such that $a+b+c=0$, then we define a subgroup $\Gamma_{a,b,c} \subset G$ by

$$\Gamma_{a,b,c} = \left\{(\zeta_1,\zeta_2,\zeta_3) : \zeta_1^a\zeta_2^b\zeta_3^c = 1\right\}/\text{ diagonal}\,.$$

We set $F_{a,b,c} = F_{\Gamma_{a,b,c}}$. Then $F_{a,b,c}$ has positive genus if and only if $p \nmid abc$. Clearly $F_{a,b,c}$ depends only on a, b, and c modulo p. We choose a and b in their congruence classes so that $a \geqslant 0$ and $b \geqslant 0$. Then $F_{a,b,c}$ has affine equation

$$y^p = (-1)^c x^a (1-x)^b, \tag{2}$$

and the map $\theta_{a,b,c} : F \to F_{a,b,c}$ is given by the equations

$$(X,Y,Z) \mapsto (x,y) = \left(X^pZ^{-p}, X^aY^b(-Z)^c\right).$$

There is a proper model $\mathcal{F}_{a,b,c}$ for $F_{a,b,c}$ with good reduction outside p to which γ extends, so by functoriality of the Brauer group,

$$\theta_{a,b,c}\left(F(\mathbb{A}_{\mathbb{Q},S})^{\mathrm{Br}_S(\mathcal{F})}\right) \subset F_{a,b,c}(\mathbb{A}_{\mathbb{Q},S})^{\mathrm{Br}_S(\mathcal{F}_{a,b,c})} \tag{3}$$

for any set S of primes containing p.

https://doi.org/10.1017/S0004972700019493 Published online by Cambridge University Press

THEOREM B. *In addition to the hypotheses of Theorem A, let* $\gamma = a^a b^b c^c$ *and suppose that*

$$\gamma^p \not\equiv \gamma \pmod{p^2}. \tag{4}$$

Then

$$\left|F_{a,b,c}(\mathbb{Q}_p)^{\mathrm{Br}_S(\mathcal{F}_{a,b,c})}\right| \leqslant p.$$

Furthermore, there exists a quotient curve $F_{a,b,c}$ *such that (4) is satisfied.*

In view of (3), Theorem A follows from Theorem B.

The basic method used in proving Theorems A and B is the same as that used in [10], but the connection between that method and Brauer-Manin obstruction was not dealt with there. Although the bound on rational points in [10] is now obsolete, the question of whether the rational points coincide with the Brauer points remains open; either an affirmative or a negative answer would be interesting. The bound given here is stronger than the one given in [10] because of the explicit computation of Coleman integrals given in Section 4.

2. Outline of the Proof

Let X be a complete proper curve over a field K, with a rational base point $O \in X(K)$. Let J be the jacobian of X, and let $j : X \hookrightarrow J$ be the embedding which takes O to the identity element, e. Let $\mathrm{Br}_0(X)$ be the image of $\mathrm{Br}(K)$ in $\mathrm{Br}(X)$ coming from the map $X \to \mathrm{spec}(K)$. Then, as explained in [8], there is an exact sequence

$$0 \to \mathrm{Br}(X)/\mathrm{Br}_0(X) \to H^1(K, \mathrm{Pic}\,\overline{X}) \to H^3\left(K, \overline{K}^\times\right).$$

Since $X(K) \neq \emptyset$, we have an isomorphism

$$H^1(K, J) \simeq H^1(K, \mathrm{Pic}\,\overline{X}).$$

Furthermore, if K is a number field or a completion of a number field, then $H^3\left(K, \overline{K}^\times\right) = 0$, so we get an isomorphism

$$\phi\colon H^1(K, J) \simeq \mathrm{Br}(X)/\mathrm{Br}_0(X).$$

It is shown in [8] that if K is a local field, $d \in H^1(K, J)$, $x \in X(K)$, then

$$\mathrm{inv}_v\big(\phi(d)(x)\big) - \mathrm{inv}_v\big(\phi(d)(O)\big) = \langle j(x), d\rangle$$

where $\langle\ ,\ \rangle$ is the Tate local pairing

$$J(K) \times H^1(K, J) \to \mathbb{Q}/\mathbb{Z}.$$

https://doi.org/10.1017/S0004972700019493 Published online by Cambridge University Press

Suppose now that K is a number field, S an inequivalent set of valuations of K, and define $Ш_S(K,J)$ by exactness of the sequence

$$0 \to Ш_S(K,J) \to H^1(K,J) \to \prod_{v \notin S} H^1(K_v,J).$$

LEMMA 1. *Suppose S contains at least one non-archimedean valuation, and let $\mathcal{X}$ be a proper model for X over $\mathcal{O}_K$. Then $\phi\big(Ш_S(K,J)\big)$ is contained in the image of $\mathrm{Br}_S(\mathcal{X})$ in $\mathrm{Br}(X)/\mathrm{Br}_0(X)$.*

PROOF: Let $d \in Ш_S(K,J)$, and let $a \in \mathrm{Br}(X)$ be an element representing the class of $\phi(d)$. Since $d_v = 0$ for all $v \notin S$, a_v is contained in $\mathrm{Br}_0(X_v)$ for all $v \notin S$. Furthermore, since S contains a non-archimedean valuation, there exists an element $b \in \mathrm{Br}(K)$ such that $a_v = b_v$ for all $v \notin S$. Then $a - b$ represents the same class as a and is contained in $\mathrm{Br}_S(\mathcal{X})$. □

Thus, if we define

$$J(\mathbb{A}_{K,S})^{Ш_S(K,J)} = \left\{ x \in J(\mathbb{A}_{K,S}) : \sum_{v \in S} \langle x, d_v \rangle_v = 0 \quad \forall\, d \in Ш_S(K,J) \right\},$$

then

$$j\big(X(\mathbb{A}_{K,S})^{\mathrm{Br}_S(\mathcal{X})}\big) \subset J(\mathbb{A}_{K,S})^{Ш_S(K,J)}. \tag{5}$$

Now, let p be an odd prime number and let $X = F_{a,b,c}$, embedded in its jacobian J via the base point $O = (0,0)$. Let $\mathcal{F}_{a,b,c}$ be the model for $F_{a,b,c}$ obtained by taking the normalisation of the projective completion of the affine curve over $\mathbb{Z}_p$ defined by the equation (2). Then $\mathcal{F}_{a,b,c}$ has good reduction outside p.

Let $K = \mathbb{Q}(\zeta_p)$, and let C be the ideal class group of K. In Section 3 we shall prove the following proposition.

PROPOSITION 2. *Suppose that $\mathrm{rank}_{\mathbb{Z}/p\mathbb{Z}}(C/pC) < (p+3)/8$, and let $S = \{v_p\}$. Then there exists $\big(\mathbf{d}^{(n)}\big) \in \varprojlim_n Ш_S(\mathbb{Q},J)[p^n]$ such that $\left(\mathbf{d}_p^{(n)}\right)$, the localisation at p, is not zero.*

Let $B \subset J(\mathbb{Q}_p) = J(\mathbb{A}_S)$ be the subgroup cut out by $\mathbf{d}$. Then it follows from (5) that

$$j\big(F_{a,b,c}(\mathbb{Q}_p)^{\mathrm{Br}_S(\mathcal{F}_{a,b,c})}\big) \subset B. \tag{6}$$

Let

$$\Lambda : J(\mathbb{Q}_p) \to T_e\big(J(\mathbb{Q}_p)\big)$$

https://doi.org/10.1017/S0004972700019493 Published online by Cambridge University Press

be the logarithm map for $J(\mathbb{Q}_p)$ as a p-adic Lie group (see [2], Section 7.6). It follows from the fact that $\mathbf{d}_p \neq 0$ that B has positive codimension in $J(\mathbb{Q}_p)$. Hence $\Lambda\big(J(\mathbb{Q}_P)\big)$ has positive codimension $T_e\big(J(\mathbb{Q}_p)\big)$. Thus we may choose a non-zero element $\omega \in H^0\big(J_{\mathbb{Q}_p}, \Omega^1\big)$, the dual $\mathbb{Q}_p$-vector space to $T_e\big(J(\mathbb{Q}_p)\big)$, such that the composite

$$\lambda_\omega : J(\mathbb{Q}_p) \xrightarrow{\Lambda} T_e\big(J(\mathbb{Q}_p)\big) \xrightarrow{\omega} \mathbb{Q}_p$$

vanishes on $j\Big(F_{a,b,c}(\mathbb{Q}_p)^{\mathrm{Br}\,S\,(\mathcal{F}_{a,b,c})}\Big)$.

For η, a holomorphic differential on $F_{a,b,c}$ or on J, defined over $\mathbb{C}_p$, let

$$\lambda_\eta(P) = \int_{(0,0)}^{P} \eta$$

be the integral of η in the sense of Coleman [5]. (It exists since $F_{a,b,c}$ has potential good reduction.) It is shown in [5] that there is no conflict in notation here: λ_ω as defined above using the logarithm is the same as the Coleman integral of ω. Let $\eta = j^*\omega$, and let λ_η be the integral of η on $F_{a,b,c}$. By functoriality of the integral, if follows from (6) that

$$\lambda_\eta\Big(F_{a,b,c}(\mathbb{Q}_p)^{\mathrm{Br}\,S\,(\mathcal{F}_{a,b,c})}\Big) = 0. \tag{7}$$

As explained in [10], (7) already implies that $F_{a,b,c}(\mathbb{Q}_p)^{\mathrm{Br}\,S}$ has cardinality at most $2p-3$. To do better than that, we find in Section 4 a basis for $H^0\big(J_{\mathbb{Q}_p}, \Omega^1\big)$ whose elements we can integrate explicitly on a certain affinoid contained in $F_{a,b,c}(\mathbb{C}_p)$.

We say (for reasons to do with the associated Jacobi-sum Hecke character) that $F_{a,b,c}$ is *wild* if (4) is satisfied, and *tame* otherwise. The special fibre of $\mathcal{F}_{a,b,c}$ has a cusp at the point ξ where $\widetilde{x}(\xi) = -\widetilde{a}/\widetilde{c}$, and no other singularities. If $F_{a,b,c}$ is wild, then $\mathcal{F}_{a,b,c}$ is regular [11]. In this case, let $\mathbb{X} \subset F_{a,b,c}(\mathbb{C}_p)$ be the affinoid reducing to the special fibre of $\mathcal{F}_{a,b,c}$ with the cusp deleted. Since every $\mathbb{Q}_p$ rational point on $F_{a,b,c}$ reduces to a nonsingular point on the special fibre of $\mathcal{F}_{a,b,c}$, $F_{a,b,c}(\mathbb{Q}_p) \subset \mathbb{X}$.

PROPOSITION 3. *Let η be a non-zero holomorphic differential on $F_{a,b,c}$, defined over $\mathbb{C}_p$. Suppose that $F_{a,b,c}$ is wild. Then λ_η has at most p zeros in $\mathbb{X}$.*

It is shown in [11, Lemma 4.7] that there exists a, b, c such that $F_{a,b,c}$ is wild. Then (7) implies Theorem B, and hence Theorem A. It remains to prove Propositions 2 and 3.

3. Construction of an Element of the Brauer Group

In this section we prove Proposition 2. Since $F_{a,b,c}$ has an automorphism $y \mapsto \zeta_p y$, where ζ_p is a primitive p-th root of unity, J has complex multiplication by $\mathbb{Z}[\zeta_p]$, hence

https://doi.org/10.1017/S0004972700019493 Published online by Cambridge University Press

an endomorphism $\pi = 1 - \zeta_p$. Let $K = \mathbb{Q}(\zeta)$, let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$, and let $\mathfrak{p}$ be the prime of K lying above p. We claim that in order to construct the element $\mathbf{d}$ in the conclusion of Proposition 2, it suffices to construct an element $\mathbf{d}' \in \varprojlim_n Ш_S(K,J)[\pi^n]$, $S = \{v_\mathfrak{p}\}$, whose localisation at $\mathfrak{p}$ is non-zero. We see this as follows: First, since $\pi^{p-1} \simeq p$ in $\mathcal{O}_K$, there is an isomorphism $\varprojlim_n Ш_S(K,J)[\pi^n] \simeq \varprojlim_n Ш_S(K,J)[p^n]$. Hence from $\mathbf{d}'$ we get an element $\mathbf{d}'' \in \varprojlim_n Ш_S(K,J)[p^n]$ locally non-zero at $\mathfrak{p}$. Second by applying a suitable idempotent from the group algebra $\mathbb{Z}_p[\Delta]$ we may assume $\mathbf{d}''$ is an eigenvector for the action of $\mathrm{Gal}(K/\mathbb{Q})$ and locally non-zero at $\mathfrak{p}$. Finally, the complex multiplication gives a natural action of $\mathbb{Z}_p[\zeta]$ on $\varprojlim_n Ш(K,J)[p^n]$. Let $\varpi = (-p)^{1/(p-1)} \in \mathbb{Z}_p[\zeta]$. Then the action of Δ on ϖ is given by the cyclotomic character, so, multiplying $\mathbf{d}''$ by a suitable power of ϖ we get an element fixed by Δ. Since the order of Δ is prime to p, this element is the restriction of an element $\mathbf{d} \in \varprojlim_n Ш(\mathbb{Q},J)[p^n]$ as required.

Now, let K_S be the maximal extension of K which is unramified outside $\mathfrak{p}$, and let $G_S = \mathrm{Gal}(K_S/K)$. Since J has good reduction outside S, $Ш_S(K,J) = H^1\big(K_S/K, J(K_S)\big)$. The Kummer sequence

$$0 \to J[\pi^n] \to J(K_S) \xrightarrow{\pi^n} J(K_S) \to 0$$

yields a surjective map

$$H^1\big(K_S/K, J[\pi^n]\big) \twoheadrightarrow H^1\big(K_S/K, J(K_S)[\pi^n]\big),$$

so to construct $\mathbf{d}' \in \varprojlim_n Ш_S(K,J)[\pi^n]$, we construct $\mathbf{c} \in \varprojlim_n H^1\big(K_S/K, J[\pi^n]\big)$. For each n we have an exact sequence of G_S-modules

$$0 \to J[\pi^n] \to J[\pi^{n+1}] \xrightarrow{\pi^n} J[\pi] \to 0.$$

Let

$$\delta_n : H^1\big(K_S/K, J[\pi]\big) \to H^2\big(K_S/K, J[\pi^n]\big)$$

be the associated coboundary map. Also, let

$$\delta_\mathfrak{p} : J(K_\mathfrak{p})/\pi J(K_\mathfrak{p}) \to H^1\big(K_\mathfrak{p}, J[\pi]\big)$$

be the coboundary of the sequence

$$0 \to J[\pi] \to J\big(\overline{K}_\mathfrak{p}\big) \xrightarrow{\pi} J\big(\overline{K}_\mathfrak{p}\big) \to 0.$$

To construct $\mathbf{c}$, it suffices to show there is an element $\mathbf{c}^{(1)} \in H^1\big(K_S/K, J[\pi]\big)$ such that

$$\delta_n \mathbf{c}^{(1)} = 0 \quad \forall n > 0. \tag{8}$$

https://doi.org/10.1017/S0004972700019493 Published online by Cambridge University Press

and

$$\mathbf{c}_{\mathfrak{p}}^{(1)} \notin \operatorname{im}\delta_{\mathfrak{p}}. \tag{9}$$

Indeed, (8) implies that $\mathbf{c}^{(1)}$ can be lifted to $\mathbf{c}^{(n)} \in H^1\big(K_S/K, J[\pi^n]\big)$ for arbitrarily large n, and, since the groups $H^1\big(K_S/K, J[\pi^n]\big)$ are finite, this implies that there is a compatible sequence of such $c^{(n)}$. The images of these in $H^1(K_S/K, J)[\pi^n]$ give an element $\big(\mathbf{d}^{(n)}\big) \in \varprojlim Ш_S(K, J)[\pi^n]$, and condition (9) ensures that $\mathbf{d}_{\mathfrak{p}} \neq 0$.

LEMMA 4. *We have*

$$\dim_{\mathbf{Z}/p\mathbf{Z}}\Big(\bigcap_{n>0} \ker\delta_n\Big) \geqslant \dim_{\mathbf{Z}/p\mathbf{Z}} H^1(K_S/K, J[\pi]) - \dim_{\mathbf{Z}/p\mathbf{Z}} H^2\big(K_S/K, J[\pi]\big).$$

PROOF: Let $\delta'_n : H^1\big(K_S/K, J[\pi^n]\big) \to H^2\big(K_S/K, J[\pi]\big)$ be the coboundary of the sequence

$$0 \to J[\pi] \to J[\pi^{n+1}] \to J[\pi^n] \to 0.$$

Consider the diagram

$$\begin{array}{ccc} H^1\big(K_S/K, J[\pi]\big) & \xrightarrow{\delta_n} & H^2\big(K_S/K, J[\pi^n]\big) \\ & \searrow^{\delta_{n+1}} & \uparrow{\scriptstyle \pi_*} \\ & & H^2\big(K_S/K, J[\pi^{n+1}]\big) \\ & & \uparrow \\ & & H^2\big(K_S/K, J[\pi]\big) \\ & & \uparrow{\scriptstyle \delta'_n} \\ & & H^1\big(K_S/K, J[\pi^n]\big) \end{array}$$

The groups $\ker\delta_n$ form a descending filtration on $H^1\big(K_S/K, J[\pi]\big)$ with intersection H, say. Further, δ_{n+1} restricted to $\ker\delta_n$ maps to the image of $H^2\big(K_S/K, J[\pi]\big)$ in $H^2\big(K_S/K, J[\pi^{n+1}]\big)$, which is $H^2\big(K_S/K, J[\pi]\big)/\operatorname{im}\delta'_n$. Thus we get a series of induced maps for $n \geqslant 0$

$$\delta^*_{n+1} : \ker\delta_n \to H^2\big(K_S/K, J[\pi]\big)/\operatorname{im}\delta'_n,$$

where we adopt the convention that $\ker\delta_0 = H^1\big(K_S/K, J[\pi]\big)$ and $\operatorname{im}\delta'_0 = \{0\}$. Further, it is easy to see that $\ker\delta^*_n = \ker\delta_n$, and with a little more thought one can see

that $\operatorname{im}\delta_n^* = \operatorname{im}\delta_n'/\operatorname{im}\delta_{n-1}'$. The images $\operatorname{im}\delta_n'$ eventually stabilise on some subgroup $\operatorname{im}\delta_\infty'$, and by summing dimensions over n we find that

$$\dim\Big(H^1\big(K_S/K, J[\pi]\big)/H\Big) = \sum_{n=0}^{\infty} \dim\left(\ker\delta_n/\ker\delta_{n+1}\right) = \sum_{n=0}^{\infty} \dim\left(\operatorname{im}\delta_{n+1}'/\operatorname{im}\delta_n'\right)$$
$$= \dim\operatorname{im}\delta_\infty' \leqslant \dim H^2\big(K_S/K, J[\pi]\big). \qquad \square$$

To describe $\delta_{\mathfrak{p}}\big(J(K_{\mathfrak{p}})\big)$, it is convenient to choose an isomorphism of Galois modules $J[\pi] \simeq \mu_p$, inducing an isomorphism

$$\iota_{\mathfrak{p}} : H^1\big(K_{\mathfrak{p}}, J[\pi]\big) \simeq H^1(K_{\mathfrak{p}}, \mu_p) = K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*p}.$$

For $i > 0$, let U_i be the image of $1 + \pi^i\mathcal{O}_{\mathfrak{p}}$ in $K_{\mathfrak{p}}/K_{\mathfrak{p}}^{\times p}$, and let $U_0 = K_{\mathfrak{p}}/K_{\mathfrak{p}}^{\times p}$.

THEOREM 5. (Faddeev [6, Theorem 4)] We have

$$U_{(p+3)/2} \subset (\iota_{\mathfrak{p}} \circ \delta)\big(J(K_{\mathfrak{p}})\big) \subset U_{(p-1)/2}.$$

Furthermore, each containment is strict.

Let $\ell_{\mathfrak{p}}$ be the localisation map

$$\ell_{\mathfrak{p}} : H^1\big(K_S/K, J[\pi]\big) \to H^1\big(K_{\mathfrak{p}}, J[\pi]\big).$$

LEMMA 6. *The isomorphism $J[\pi] \simeq \mu_p$ induces isomorphisms*

$$\iota_1 : H^1\big(K_S/K, J[\pi]\big) \simeq H^1(K_S/K, \mu_p) = \big\{x \in K^*/K^{*p} : v(x) \equiv 0 \pmod p,\ v \neq v_{\mathfrak{p}}\big\},$$
$$\iota_2 : H^2\big(K_S/K, J[\pi]\big) \simeq H^2(K_S/K, \mu_p) = C/pC.$$

Furthermore, the image of $H^1(K_S/K, \mu_p)$ in $H^1(K_{\mathfrak{p}}, \mu_p)$ is a maximal isotropic subgroup for the local Hilbert pairing.

PROOF: The isomorphisms may be obtained by considering cohomology of the exact sequence

$$0 \to \mu_p \to \mathcal{O}_{K_S}{}^{\times} \xrightarrow{p} \mathcal{O}_{K_S}{}^{\times} \to 0$$

or by identifying the Galois cohomology groups with étale cohomology groups and taking cohomology of the Kummer sequence

$$0 \to \mu_p \to \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}} \to 0$$

of étale sheaves on $\operatorname{Spec}\big(\mathcal{O}_K[1/p]\big)$. Note that the class group of $\mathcal{O}_K[1/p]$ is the same as the class group of $\operatorname{Spec}(\mathcal{O})$, since $\mathfrak{p}$ is principal, and that $\mathfrak{p}$ is the only prime of

https://doi.org/10.1017/S0004972700019493 Published online by Cambridge University Press

K above p, so that the Brauer group of $\mathcal{O}_K[1/p]$ is trivial. The last statement is a straightforward application of Tate global duality. □

LEMMA 7. *We have*

$$\dim\left(\ell_{\mathfrak{p}}^{-1}(\operatorname{im}\delta_{\mathfrak{p}})\right) \leqslant \dim H^1\left(K_S/K, J[\pi]\right) + \dim C/pC - (p+3)/4.$$

PROOF: We have

$$\dim\left(\ell_{\mathfrak{p}}^{-1}(\operatorname{im}\delta_{\mathfrak{p}})\right) = \dim\ker\ell_{\mathfrak{p}} + \dim\left(\operatorname{im}\ell_{\mathfrak{p}} \cap \operatorname{im}\delta_{\mathfrak{p}}\right).$$

By Lemma 6 and the fact that $\dim K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times p} = p+1$, we have

$$\dim\ker\ell_{\mathfrak{p}} = \dim H^1\left(K_S/K, J[\pi]\right) - (p+1)/2. \tag{10}$$

From Theorem 5 we have $\dim\operatorname{im}\delta_{\mathfrak{p}} = (p+1)/2$. We claim that

$$\dim\left(\operatorname{im}\ell_{\mathfrak{p}} \cap \operatorname{im}\delta_{\mathfrak{p}}\right) \leqslant (p-1)/4 + \dim\left(C/pC\right). \tag{11}$$

This follows from the fact that U_i and U_j pair nontrivially with respect to the Hilbert pairing if $i+j=p$, trivially if $i+j>p$. Since $\operatorname{im}\ell_{\mathfrak{p}}$ is isotropic with respect to the Hilbert pairing and $\operatorname{im}\delta_{\mathfrak{p}} \supset U_{(p+3)/2}$, the dimension of $\operatorname{im}\ell_{\mathfrak{p}} \cap \operatorname{im}\delta_{\mathfrak{p}}$ is decreased by 1 from $\dim\operatorname{im}\delta_{\mathfrak{p}}$ for each $i \leqslant (p-3)/2$ such that there exists $\eta \in H^1(K_S/K, \mu_p)$ with $\eta_{\mathfrak{p}} \in U_i \setminus U_{i+1}$. For $i = 0, 1$ we may choose $\eta = \pi, \zeta$ respectively. If i is even and less than $(p-1)/2$ and if $p \nmid B_i$, the i-th Bernoulli number, then we may choose η to be the cyclotomic unit

$$\prod_{a\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\zeta^{a/2} - \zeta^{-a/2}\right)^{a^i},$$

(see [**14**, Proposition 8.12]). Thus

$$\begin{aligned}\dim\left(\operatorname{im}\ell_{\mathfrak{p}} \cap \operatorname{im}\delta_{\mathfrak{p}}\right) &\leqslant \frac{p+1}{2} - 2 - \#\left\{B_{2k} : 2k < (p-1)/2,\ p \nmid B_{2k}\right\} \\ &\leqslant \frac{p-3}{2} - \left[\frac{p-3}{4}\right] + i(p) \\ &\leqslant \frac{p-1}{4} + i(p),\end{aligned}$$

where $i(p)$ is the index of irregularity of p, that is, the number of Bernoulli numbers B_{2k}, $2 \leqslant 2k \leqslant p-1$ such that $p \mid B_{2k}$. Finally, (11) follows from the fact that, by Ribet's converse to Herbrand's theorem [**12**],

$$i(p) \leqslant \operatorname{rank}_{\mathbf{Z}/p\mathbf{Z}}\left(C/pC\right).$$

The lemma now follows from adding (10) and (11). □

PROOF OF PROPOSITION 2: We want to show that there is an element $\mathbf{c}^{(1)} \in H^1(K_S/K, J[\pi])$ contained in $\bigcap_n \ker \delta_n$ but not contained in $\ell_{\mathfrak{p}}^{-1}(\operatorname{im}\delta_{\mathfrak{p}})$. This will follow if $\dim\left(\bigcap_n \ker\delta_n\right) > \dim\left(\ell_{\mathfrak{p}}^{-1}(\operatorname{im}\delta_{\mathfrak{p}})\right)$. By Lemmas 7 and 6,

$$\dim\left(\bigcap_n \ker\delta_n\right) \geqslant \dim H^1(K_S/K, J[\pi]) - \dim C/pC$$

and by Lemma 4

$$\dim\left(\ell_{\mathfrak{p}}^{-1}(\operatorname{im}\delta_{\mathfrak{p}})\right) \leqslant \dim H^1(K_S/K, J[\pi]) + \dim C/pC - (p+3)/4. \qquad \square$$

4. COMPUTATION OF THE INTEGRALS

Consider the model $\mathcal{F} \subset \mathbb{P}^2_{\mathbb{Z}_p}$ for F given by the equation

$$X^p + Y^p = Z^p,$$

and the model $\mathcal{F}_{a,b,c}$ for $F_{a,b,c}$ given by the normalisation of the projective completion of the affine curve over $\mathbb{Z}_p$ with equation

$$y^p = (-1)^c x^a (1-x)^b.$$

PROPOSITION 8. *The special fibre of $\mathcal{F}_{a,b,c}$ is a curve of geometric genus zero with one singularity, a cusp, at the point ξ with maximal ideal*

$$\mathfrak{m}_\xi = \left(x + \frac{a}{c}, y + a^a b^b c^c, p\right). \tag{12}$$

In terms of the coordinates s and t defined by

$$x = \frac{-a}{c}(1+s), \qquad y = a^a b^b c^c (1+t), \tag{13}$$

the cusp is at $\tilde{s} = 0$, $\tilde{t} = 0$, and the special fibre has equation

$$\tilde{t}^p = \frac{ac}{2b}\tilde{s}^2\psi(\tilde{s}), \qquad \psi \in \mathbb{Z}[\tilde{s}],\ \psi(0) = 1 \tag{14}$$

in an affine neighbourhood of the cusp. Furthermore, if $F_{a,b,c}$ is wild, then $\mathcal{F}_{a,b,c}$ is the minimal regular model for $F_{a,b,c}$ over $\mathbb{Z}_p$.

PROOF: The final statement is [**11,** Proposition 6.1]. The rest is simple direct calculation. We note only that the fact that the cusp has arithmetic genus $(p-1)/2$,

https://doi.org/10.1017/S0004972700019493 Published online by Cambridge University Press

equal to the genus of $F_{a,b,c}$, provides a simple way of proving that it is the only singularity on the reduction; however, this can also be seen by performing the normalisation of $F_{a,b,c}$ explicitly. □

In what follows, we consider $F_{a,b,c}$ as an object in the rigid analytic category over $\mathbb{C}_p$, the completion of the algebraic closure of $\mathbb{Q}_p$. For general facts about rigid analysis, we refer the reader to [1]. We assume throughout that $F_{a,b,c}$ is wild. Let $\mathbb{X}$ be the affinoid in $F_{a,b,c}$ reducing to the nonsingular locus of $\widetilde{\mathcal{F}}_{a,b,c}$. Since $\widetilde{\mathbb{X}}$ is isomorphic to the affine line, $\mathbb{X}$ is isomorphic over $\mathbb{C}_p$ to a closed p-adic disc [1, 6.4.2, Corollary 3, and 3.6, Proposition 12]. Our aim in this section is to calculate the integral on the affinoid $\mathbb{X}$ of a general differential ω.

Let $O_0 = (0,0)$, $O_1 = (1,0)$, and $O_\infty = \infty$. Recall from [11, Lemma 7.2] that there exists a rigid analytic isomorphism $T\colon \mathbb{X} \simeq \mathbb{B}[1]$, defined over $\mathbb{Q}_p$, such that

$$T(O_0) = 0, \quad T(O_1) = 1, \quad T(O_\infty) = -\frac{b}{c}.$$

Let $\mathfrak{m}$ be the maximal ideal in the ring of integers of $\mathbb{C}_p$. If η is a holomorphic differential on $\mathbb{X}$ whose expansion in T has integer coefficients, we write $\widetilde{\eta}$ for its reduction modulo $\mathfrak{m}$. Any differential may be multiplied by a constant so that $\widetilde{\eta}$ is defined and not zero. We recall the following proposition from [11, Proposition 8.5].

PROPOSITION 9. *Let η be a holomorphic differential on $F_{a,b,c}$, defined over $\mathbb{C}_p$, and let λ_η be the Coleman integral of η satisfying $\lambda_\eta(O_0) = 0$. Then λ_η is analytic on $\mathbb{X}$. Further, if $\widetilde{\eta}$ is defined and not zero, then $\widetilde{\lambda}$ is the unique polynomial in $\widetilde{T}$ such that*

$$d\widetilde{\lambda} = \widetilde{\eta}, \tag{15}$$

$$\widetilde{\lambda}\left(\widetilde{T}\right) = \mu\left(\widetilde{T}\right) + \alpha\widetilde{T}^p + \beta\widetilde{T}^{2p}, \quad \mu \in \overline{\mathbb{F}}_p[\widetilde{T}],\ \deg\mu \leqslant p-2,\ \alpha,\beta \in \overline{\mathbb{F}}_p\ , \tag{16}$$

and

$$\lambda(0) = \lambda(1) = \lambda(-b/c) = 0. \tag{17}$$

PROOF OF PROPOSITION 9: We apply Proposition 3 to the following basis of holomorphic differentials. If $z \in \mathbb{Q}$, let $[z]$ denote the integer part of z. Let

$$H_{a,b,c} = \left\{k : 1 \leqslant k \leqslant p-1,\ \left[\frac{ka}{p}\right] + \left[\frac{kb}{p}\right] + \left[\frac{kc}{p}\right] = -2\right\}.$$

For $k \in H_{a,b,c}$, let

$$\eta_k = \frac{x^{[ka/p]}(1-x)^{[kb/p]}}{y^k}\,dX.$$

https://doi.org/10.1017/S0004972700019493 Published online by Cambridge University Press

The set $\{\eta_k : k \in H_{a,b,c}\}$ is a basis for the space of holomorphic differentials on $F_{a,b,c}$, each element of which is an eigenvector for the complex multiplication action.

If $m \in \mathbb{Z}$, let $r(m)$ denote the unique residue of $m \pmod p$ such that $0 \leqslant r(m) \leqslant p-1$. Then [9]

$$\begin{aligned} \operatorname{ord}_{(0,0)}(\eta_k) &= p-1-r(ka), \\ \operatorname{ord}_{(0,1)}(\eta_k) &= p-1-r(kb), \\ \operatorname{ord}_{\infty}(\eta_k) &= p-1-r(kc), \end{aligned}$$

and η_k has no other zeros. It follows that, on $\mathbb{X}$,

$$\eta_k = \text{constant} \times u(T) \times T^{p-1-r(ka)}(T-1)^{p-1-r(kb)}\left(T+\frac{b}{c}\right)^{p-1-r(kc)} dT, \tag{18}$$

where $u(T)$ has constant term 1 and all other coefficients in $\mathfrak{m}$. Replace η_k by a suitable multiple so that the constant in (18) is 1. We claim that

$$\widetilde{\lambda}_{\eta_k} = T^{p-r(ka)}(T-1)^{p-r(kb)}\left(T+\frac{b}{c}\right)^{p-r(kc)}. \tag{19}$$

First, note that the coefficient of T^{p-1} in the expression on the right is

$$-\big(p-r(kb)\big)+\big(p-r(kc)\big)\frac{b}{c} \equiv kb - kc\frac{b}{c} = 0 \pmod p.$$

Thus $\widetilde{\lambda}_{\eta_k}$ has the form (16). Therefore, $d\widetilde{\lambda}_{\eta_k} = f(T)\,dT$ for some polynomial of degree at most $p-3$; on the other hand, $f(T)$ has a zero of the same order as $\widetilde{\eta}_k$ at $T = 0, 1, -b/c$, and the sum of these orders is $2g-2 = p-3$, hence $f(T)\,dT = \widetilde{\eta}_k$ with a suitable choice of the constant. Thus, $\widetilde{\lambda}_{\eta_k}$ satisfies (15). Finally, it clearly satisfies (17) and our claim follows from Proposition 9.

We have shown that for each η_k, $\widetilde{\lambda}_k(T)$ is a polynomial in T of degree at most p. Now let η be any holomorphic differential. Since the η_k form a basis for the holomorphic differentials, some multiple of η is an integral linear combination of the η_k, with at least one of the coefficients a unit. Therefore $\widetilde{\lambda}_\eta$ is a non-trivial linear combination of the polynomials (19). It is not hard to see that these polynomials are linearly independent (by noting that they all have different orders of vanishing at $T = 0$, for example). Thus $\widetilde{\lambda}_\eta$ is a non-zero polynomial in T of degree at most p. Proposition 3 now follows from the theory of analytic functions on a closed p-adic disc (see, for example, [7]). □

Although it is not needed for results in this paper, we remark in conclusion that if $\eta = \eta_k$, then λ_η vanishes only at the three points O_0, O_1 and ∞. Indeed, it must vanish at those points, because they are torsion points on the jacobian. On the other

https://doi.org/10.1017/S0004972700019493 Published online by Cambridge University Press

hand, it follows from (19) that λ_η has $p-r(a)$ zeros in the residue class of O_0, $p-r(b)$ zeros in the residue class of O_1, and $p-r(c)$ zeros in the residue class of O_∞, and no other zeros on $\mathbb{X}$. Further, since it vanishes at O_0, O_1, and O_∞, it follows from (18) that it vanishes to order $p-r(a)$, $p-r(b)$, and $p-r(c)$, respectively. Therefore, its only zeros are at those three points.

References

[1] S. Bosch, U. Guntzer and R. Remmert, *Non-archimedean analysis* (Springer-Verlag, Berlin, Heidelberg, New York, 1984).

[2] N. Bourbaki, *Lie groups and Lie algebras, Part I* (Hermann, Addison-Wesley, Reading, MA, 1975).

[3] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä and M.A. Shokrollahi, 'Irregular primes and cyclotomic invariants to twelve million', *J. Symbolic Comput.* **31** (2001), 89–96.

[4] L. Carlitz, 'A generalization of Maillet's determinant and a bound for the first factor of the class number', *Proc. Amer. Math. Soc.* **12** (1961), 256–261.

[5] R.F. Coleman, 'Torsion points on curves and p-adic abelian integrals', *Ann. of Math.* **121** (1983), 111–168.

[6] 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.

[7] J. Fresnel and M. van der Put, *Géometrie analytique rigide et applications*, Progress in Mathematics **18** (Birkhäuser, Boston, Basel, Stuttgart, 1981).

[8] Y.I. Manin, 'Le groupe de Brauer-Grothendieck en géométrie diophantienne', in *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1* (Gauthier-Villars, Paris, 1971), pp. 401–411.

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

[10] W.G. McCallum, 'The arithmetic of Fermat curves', *Math. Ann.* **294** (1992), 503–511.

[11] W.G. McCallum, 'The method of Coleman and Chabauty', *Math. Ann.* **299** (1994), 565–596.

[12] K. Ribet, 'On modular representations of Gal $(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms', *Invent. Math.* **100** (1990), 431–476.

[13] V. Scharaschkin, 'The Brauer-Manin obstruction for curves', (preprint).

[14] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics **83** (Springer-Verlag, Berlin, Heidelberg, New York, 1982).

Department of Mathematics
University of Arizona
Tucson, AZ 85721
United States of America