BRAUER POINTS ON FERMAT CURVES

William G. McCallum
August, 2000

In honor of George Szekeres on his 90th birthday

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 [Man] 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*

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

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 [Sch, 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 $\tilde{a}_v \in \mathrm{Br}(\mathcal{X}_v)$ such that $a_v = j^*(\tilde{a}_v)$, and since $\mathcal{X}$ is proper, there is a section $\tilde{x}_v$ of $\mathcal{X}_v$ extending x_v, so $a(x_v) = a_v(x_v) = \tilde{a}_v(\tilde{x}_v) \in \mathrm{Br}(\mathcal{O}_v) = 0$. It makes sense to define the set of *S-Brauer points with respect to* $\mathcal{X}$

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

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 pth Fermat curve over $\mathbb{Q}$, with projective equation

(1)
$$X^p + Y^p = Z^p.$$

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

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

It seems quite likely that the hypothesis is always satisfied: For $p \le 12{,}000{,}000$, the largest value of the rank is 7 [BCEMS]. 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 [W], Exercise 6.6). However, the best proven bound on the rank is $\mathrm{rank}_{\mathbb{Z}/p\mathbb{Z}}(C/pC) < p/2$, which follows from a Carlitz's bound on the *size* of the minus part of the ideal class group [Ca, (21)] using the fact that the p-rank of the plus part is less than the p-rank of the minus part ([W], 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

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

2

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

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

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 $a \geq 0$ and $b \geq 0$. Then $F_{a,b,c}$ has affine equation

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

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

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

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,

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

for any set S of primes containing p.

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

$$(4) \qquad\qquad \gamma^p \not\equiv \gamma \pmod{p^2}.$$

Then

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

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 [M3], but the connection between that method and Brauer-Manin obstruction was not dealt with there. Although the bound on rational points in [M3] 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 [M3] because of the explicit computation of Coleman integrals given in Section .

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 [Man], there is an exact sequence

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

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 $H^3(K, \overline{K}^\times) = 0$, so we get an isomorphism

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

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

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

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

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

Suppose now that K is a number field, S an inequivalent set of valuations of K, and define $\mathrm{III}_S(K, J)$ by exactness of the sequence

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

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 $\phi(\mathrm{III}_S(K, J))$ is contained in the image of $Br_S(\mathcal{X})$ in $Br(X)/Br_0(X)$*

4

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

Thus, if we define

$$J(\mathbb{A}_{K,S})^{\text{III}_S(K,J)} = \{x \in J(\mathbb{A}_{K,S}) : \sum_{v \in S} \langle x, d_v \rangle_v = 0 \quad \text{for all} \quad d \in \text{III}_S(K, J)\},$$

then

(5) $$j(X(\mathbb{A}_{K,S})^{\text{Br}_S(\mathcal{X})}) \subset J(\mathbb{A}_{K,S})^{\text{III}_S(K,J)}.$$

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 normalization 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 Sect. we will prove the following proposition.

PROPOSITION **2**. *Suppose that* $\text{rank}_{\mathbb{Z}/p\mathbb{Z}}(C/pC) < (p + 3)/8$, *and let* $S = \{v_p\}$. *Then there exists* $(\mathbf{d}^{(n)}) \in \varprojlim_n \text{III}_S(\mathbb{Q}, J)[p^n]$ *such that* $(\mathbf{d}_p^{(n)})$, *the localization 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

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

Let

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

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

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

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

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

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

5

be the integral of η in the sense of Coleman [C1]. (It exists since $F_{a,b,c}$ has potential good reduction.) It is shown in [C1] 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

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

As explained in [M3], (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 Sect. a basis for $H^0(J_{\mathbb{Q}_p}, \Omega^1)$ 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 fiber of $\mathcal{F}_{a,b,c}$ has a cusp at the point ξ where $\tilde{x}(\xi) = -\tilde{a}/\tilde{c}$, and no other singularities. If $F_{a,b,c}$ is wild, then $\mathcal{F}_{a,b,c}$ is regular [M4]. In this case, let $\mathbb{X} \subset F_{a,b,c}(\mathbb{C}_p)$ be the affinoid reducing to the special fiber 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 fiber 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 zeroes in $\mathbb{X}$.*

It is shown in [M4, 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 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 $\mathbf{d}' \in \varprojlim_n \mathrm{III}_S(K, J)[\pi^n]$, $S = \{v_{\mathfrak{p}}\}$, whose localization 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 $\varprojlim_n \mathrm{III}_S(K, J)[\pi^n] \simeq \varprojlim_n \mathrm{III}_S(K, J)[p^n]$. Hence from $\mathbf{d}'$ we get an element $\mathbf{d}'' \in \varprojlim_n \mathrm{III}_S(K, J)[p^n]$ 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 $\varprojlim_n \mathrm{III}(K, J)[p^n]$. 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 $\mathbf{d} \in \varprojlim_n \mathrm{III}(\mathbb{Q}, J)[p^n]$ 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, $\mathrm{III}_S(K, J) =$

6

$H^1(K_S/K, J(K_S))$. The Kummer sequence

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

yields a surjective map

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

so to construct $\mathbf{d}' \in \varprojlim_n \mathrm{III}_S(K, J)[\pi^n]$, we construct $\mathbf{c} \in \varprojlim_n H^1(K_S/K, J[\pi^n])$. 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

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

be the associated coboundary map. Also, let

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

be the coboundary of the sequence

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

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

(8) $$\delta_n \mathbf{c}^{(1)} = 0 \qquad \text{for all} \quad n > 0.$$

and

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

Indeed, (8) implies that $\mathbf{c}^{(1)}$ can be lifted to $\mathbf{c}^{(n)} \in H^1(K_S/K, J[\pi^n])$ for arbitrarily large n, and, since the groups $H^1(K_S/K, J[\pi^n])$ 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 $(\mathbf{d}^{(n)}) \in \varprojlim \mathrm{III}_S(K, J)[\pi^n]$, and condition (9) ensures that $\mathbf{d}_{\mathfrak{p}} \neq 0$.

LEMMA **4**. *We have*

$$\dim_{\mathbb{Z}/p\mathbb{Z}}(\cap_{n>0} \ker \delta_n) \geq \dim_{\mathbb{Z}/p\mathbb{Z}} H^1(K_S/K, J[\pi]) - \dim_{\mathbb{Z}/p\mathbb{Z}} H^2(K_S/K, J[\pi]).$$

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

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

7

Consider the diagram

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

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

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

where we adopt the convention that $\ker \delta_0 = H^1(K_S/K, J[\pi])$ 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 stabilize on some subgroup $\operatorname{im} \delta'_\infty$, and summing dimensions over n we find that

$$\dim(H^1(K_S/K, J[\pi])/H) = \sum_{n=0}^{\infty} \dim(\ker \delta_n/\ker \delta_{n+1}) = \sum_{n=0}^{\infty} \dim(\operatorname{im} \delta'_{n+1}/\operatorname{im} \delta'_n)$$

$$= \dim \operatorname{im} \delta'_\infty \leq \dim H^2(K_S/K, J[\pi]).$$

∎

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

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

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

THEOREM 5 (FADDEEV [F], THEOREM 4). *We have*

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

Furthermore, each containment is strict.

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

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

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

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

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

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

Proof: We have

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

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

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

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

$$(11) \qquad \dim(\mathrm{im}\,\ell_{\mathfrak{p}} \cap \mathrm{im}\,\delta_{\mathfrak{p}}) \leq (p-1)/4 + \dim(C/pC).$$

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 $i \leq (p-3)/2$ 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

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

(see [W], Proposition 8.12). Thus

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

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

$$i(p) \leq \operatorname{rank}_{\mathbb{Z}/p\mathbb{Z}}(C/pC).$$

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 $\cap_n \ker \delta_n$ but not contained in $\ell_{\mathfrak{p}}^{-1}(\operatorname{im} \delta_{\mathfrak{p}})$. This will follow if $\dim(\cap_n \ker \delta_n) > \dim(\ell_{\mathfrak{p}}^{-1}(\operatorname{im} \delta_{\mathfrak{p}}))$. By Lemmas 4 and 6,

$$\dim(\cap_n \ker \delta_n) \geq \dim H^1(K_S/K, J[\pi]) - \dim C/pC$$

and by Lemma 7

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

∎

4. Computation of the Integrals.

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

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

10

and the model $\mathcal{F}_{a,b,c}$ for $F_{a,b,c}$ given by the normalization 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 fiber 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*

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

In terms of the coordinates s and t defined by

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

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

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

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 Proposition 6.1 of [M4]. The rest is simple direct calculation. We note only that the fact that the cusp has arithmetic genus $(p-1)/2$, 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 normalization 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 [BGR]. 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 $\tilde{\mathcal{F}}_{a,b,c}$. Since $\tilde{\mathbb{X}}$ is isomorphic to the affine line, $\mathbb{X}$ is isomorphic over $\mathbb{C}_p$ to a closed p-adic disc ([BGR], 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 [M4], 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 $\tilde{\eta}$ for its reduction modulo $\mathfrak{m}$. Any differential may be multiplied by a constant so that $\tilde{\eta}$ is defined and not zero. We recall the following proposition from [M4] (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 $\tilde{\eta}$ is defined and not zero, then $\tilde{\lambda}$ is the unique polynomial in $\tilde{T}$ such that*

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

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

and

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

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

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

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

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

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 $0 \le r(m) \le p - 1$. Then [M2]

$$\text{ord}_{(0,0)}(\eta_k) = p - 1 - r(ka),$$
$$\text{ord}_{(0,1)}(\eta_k) = p - 1 - r(kb),$$
$$\text{ord}_\infty(\eta_k) = p - 1 - r(kc),$$

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

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

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

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

12

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

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

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

We have shown that for each η_k, $\tilde{\lambda}_k(T)$ 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 $\tilde{\lambda}_\eta$ 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 $\tilde{\lambda}_\eta$ 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, [FvdP]). $\blacksquare$

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 hand, it follows from (19) that λ_η has $p - r(a)$ zeroes in the residue class of O_0, $p - r(b)$ zeroes in the residue class of O_1, and $p - r(c)$ zeroes in the residue class of O_∞, and no other zeroes 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 zeroes are at those three points.

Bibliography

[**BGR**]   S. Bosch, U. Guntzer, R. Remmert, *Non-archimedean analysis*, Springer, Berlin, 1984.

[**B**]   N. Bourbaki,, *Lie Groups and Lie Algebras, Part I*, Hermann, Addison-Wesley, Reading, Massachusetts, 1975.

[**BCEMS**]   J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, M. A. Shokrollahi, *Irregular Primes and Cyclotomic Invariants to Twelve Million*, J. Symbolic Computation **11** (1999).

[**Ca**]   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.

[**CF**]   J.W.S. Cassels, A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, London, 1967.

[**C1**]   R.F. Coleman, *Torsion points on curves and p-adic abelian integrals*, Annals of Math. **121** (1983), 111–168.

[**C2**]   _____, *Effective Chabauty*, Duke Math. J. **52** (1985), 765–770.

[**Fa**]   D.K. Faddeev, *Invariants of divisor classes for the curves $x^k(1-x) = y^l$ in an l-adic cyclotomic field*, Tr. Mat. Inst. Steklova **64** (1961), 284-293.

[**FvdP**]   J. Fresnel, M. van der Put,, *Géometrie Analytique Rigide et Applications, Progress in Mathematics, 18*, Birkhäuser, Boston, Basel, Stuttgart, 1981.

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

[**M1**] W.G. McCallum, *The degenerate fiber of the Fermat curve*, Number theory related to Fermat's last theorem (N. Koblitz, ed.), Birkhäuser, Boston, 1982.

[**M2**] _____, *On the Shafarevich-Tate group of the Jacobian of a quotient of the Fermat curve*, Invent. math. **93** (1988), 637–666.

[**M3**] _____, *The arithmetic of Fermat curves*, Math. Ann. **294** (1992), 503–511.

[**M4**] _____, *The Method of Coleman and Chabauty*, Math. Ann. **299** (1994), 565–596.

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

[**Sch**] V. Scharaschkin, *The Brauer-Manin Obstruction for Curves*, preprint.

[**W**] L.C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982.

Department of Mathematics, University of Arizona, Tucson, AZ, 85721