Terms and Conditions

Math. Ann. 299, 565–596 (1994)

Mathematische Annalen

On the method of Coleman and Chabauty *

William G. McCallum

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

Received: 2 April 1993/ In revised form: 10 February 1994

1. Introduction

Let C be a curve of genus $g \geq 2$, defined over a number field K, and let J be the Jacobian of C. Coleman [C2], following Chabauty, has shown how to obtain good bounds on the cardinality of $C(K)$ if the rank r of the Mordell-Weil group $J(K)$ is less than g. The key to the method is to construct a logarithm on $J(K_v)$, for some valuation v of K, whose kernel contains $J(K)$, and whose restriction to $C(K_v)$ is represented explicitly as the integral of a differential. This paper is an attempt to make the case, through a detailed examination of the case of Fermat curves, that this method can be fashioned into a quite precise tool for bounding rational points on curves. We show how to transform an element of the Selmer group of the Jacobian of a Fermat curve of degree p into a p-adic analytic function on the curve itself, whose zero set contains all the rational points. As a consequence, we prove the second case of Fermat's Last Theorem for regular primes. The method depends on the existence of a suitable element in the Selmer group; for the lack of a satisfactory theory of descent for Jacobians of Fermat curves, we can only show that this element exists in the case that p is regular. Of course, in that case, Kummer had already proved the whole of Fermat's Last Theorem. However, we believe the interest of this paper is in the method, not the theorem, and as such is independent of Kummer, and also of the recent work of Wiles. Our method is different, and offers a development of the method of Coleman and Chabauty, many aspects of which are generalizable to arbitrary curves, although we do not attempt to make that generalization here.

We now describe the contents of the paper in more detail. Let p be an odd prime, and let F be the p^{th} Fermat curve, with projective equation

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

* This research was supported in part by National Science Foundation grant DMS-9002095

Fermat's Last Theorem is the assertion that the only $\mathbb{Q}$-rational points on F are the trivial ones $(1,-1,0)$, $(1,0,1)$, and $(0,1,1)$. Traditionally, Fermat's Last Theorem was divided into two cases. Consider primitive solutions (x,y,z) to Eq. (1), i.e., solutions such that x, y, and z are integers with no common factor. The first case is the assertion that there are no primitive solutions such that $p \nmid xyz$; the second is that the trivial solutions are the only primitive ones such that $p|xyz$.

In [M3], we showed how the method of Chabauty and Coleman could be used to bound the number of rational points on Fermat curves under a certain hypothesis on the ideal class group of $K = \mathbb{Q}(e^{2\pi i/p})$, namely that its p-rank is less than $(p-5)/8$ (which seems likely to be the case for all p). The proof consists of two parts: a descent on the Jacobian A of F, and an application of Coleman's effective version of Chabauty's method [C2].

It is the descent that requires the hypothesis on the ideal class group. In this paper we demonstrate how more precise information from the descent, if it is available, can be used in the application of Coleman's method. We prove the second case of Fermat's Last Theorem given the existence of certain elements $d_n \in H^1(K,A)$, and we can verify the existence of these elements in the case that p is regular, i.e. the case that p does not divide the order of the ideal class group of $\mathbb{Q}(e^{2\pi i/p})$.

Before stating our theorem, we must first recast the division into cases into more geometric language. Let $\tilde{F}$ be the curve over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ obtained by reducing Eq. (1) modulo p. Then $\#(\tilde{F}(\mathbb{F}_p)) = p+1$, since the reduced curve underlying $\tilde{F}$ is isomorphic to $\mathbb{P}_1$. The second case of Fermat's Last Theorem may be reformulated as the assertion that $(1,-1,0)$, $(1,0,1)$, and $(0,1,1)$ are the only rational points in $F(\mathbb{Q})$ reducing to their respective residue classes in $\tilde{F}(\mathbb{F}_p)$. We shall call these residue classes the second case residue classes, and the remaining ones the first case residue classes. We note the following classical, and easily proved, criterion, which eliminates at least half the first case residue classes. Let $\phi \in \mathbb{Z}[T]$ be defined by

$$\phi(T) = \frac{(T+1)^p - T^p - 1}{p}.$$

Then any first case solution to Eq. (1) satisfies

$$\phi(x/y) \equiv 0 \pmod{p}.$$

Since any root of ϕ in $\mathbb{F}_p$ other than 0 and -1 must be a double root, as may be seen easily by taking the derivative, this means that at most $(p-3)/2$ first case residue classes can contain $\mathbb{Q}$-rational points (or even $\mathbb{Q}_p$-rational points).

Our main theorem depends on the existence of elements $d_n \in H^1(K,A)[p^n]$ satisfying two hypotheses (H1) and (H2). Roughly, hypothesis (H1) says that d_n is locally trivial outside p, and hypothesis (H2) says that at p it pairs non-trivially with $A(\mathbb{Q}_p)$ under Tate duality. For precise statements, see Sect. 3.

Theorem 1. *Suppose that there exist elements $d_n \in H^1(K,A)$, one for each $n \geq 0$, satisfying the hypotheses (H1) and (H2) in Sect. 3. Then there are at most p points in $F(\mathbb{Q})$. There is at most one point in each second case residue class, and at most two points in each first case residue class. Thus there are at most $p-3$ first case solutions, and no non-trivial second case solutions. In particular, the second case of Fermat's Last Theorem is true.*

At the moment, we can only verify the existence of d in the case that p is regular. We now briefly describe the proof.

First, we will in fact work mostly not with the Fermat curve itself, but with certain quotient curves. Let a, b, and c be integers such that $(abc, p) = 1$ and $a + b + c = 0$. Let $F_{a,b,c}$ be the complete nonsingular curve over $\mathbb{Q}$ with affine equation

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

There is a map of degree p

$$\begin{aligned} F &\to F_{a,b,c} \\ (X, Y, Z) &\mapsto (X^p Z^{-p}, X^a Y^b (-Z)^c), \end{aligned} \tag{3}$$

which induces a bijective map

$$F(\mathbb{Q}) \to F_{a,b,c}(\mathbb{Q}).$$

Hence bounding rational points on $F_{a,b,c}$ bounds rational points on F.

Let A be the Jacobian of $F_{a,b,c}$. The group μ_p of p-th roots of unity is contained in the automorphism group of $F_{a,b,c}$; if $\zeta \in \mu_p$ then ζ acts by

$$y \mapsto \zeta y.$$

It follows that A has potential complex multiplication by the ring of integers $\mathbb{Z}[\zeta]$, defined over $\mathbb{Q}(\zeta)$. Fix a primitive p-th root of unity ζ and let π be the endomorphism $1 - \zeta$ of A. The first part of our proof is to show by means of a π-descent that the closure of $A(\mathbb{Q})$ in $A(\mathbb{Q}_p)$ has dimension less than the dimension of $A(\mathbb{Q}_p)$ (the genus of $F_{a,b,c}$).

The second part uses Coleman's effective version of Chabauty's method. It follows from the first part that there is a non-zero holomorphic differential ω on $F_{a,b,c}$ whose Coleman integral

$$\lambda(P) = \int_O^P \omega$$

vanishes at every point of $A(\mathbb{Q})$. In particular, it vanishes at the $\mathbb{Q}$-rational points of the curve embedded in its Jacobian. In fact our descent will give some explicit information about this differential, which will enable us to compute the reduction mod p of λ on $F_{a,b,c}(\mathbb{Q}_p)$ and apply Hensel's lemma to obtain explicit bounds on the number of rational points in certain key residue classes.

Here is a brief outline of the paper. In Sect. 2 we recall some necessary background; this section may be skipped on a first reading. Sects. 3 and 4 constitute an overview of the proof, with certain rather complicated calculations omitted. In Sect. 3 we show how to bound the dimension of the closure of $A(\mathbb{Q})$ in $A(\mathbb{Q}_p)$, given the existence of a certain elements $d_n \in H^1(K, A)$. In Sect. 4 we show how to use the method of Chabauty-Coleman to deduce the main theorem, deferring the key calculation of certain differentials to Sects. 6-8. Section 5 shows the existence of d in the case that p is regular. In Sect. 6 we construct various models for Fermat curves; in Sect. 7 we find power series expansions for various functions and differentials on the Fermat curves; and in Sect. 8 we finish the calculation.

Acknowledgement. I would like to thank Greg Anderson, Robert Coleman, and Barry Mazur for their help and encouragement during the course of this work, and Jan Nekovar, Felipe Voloch, Tonghai Yang, and the anonymous referee for useful comments on the manuscript. The formulation of Sect. 3 using Proposition 4 was suggested by Robert Coleman. Part of this work was completed while I was visiting the Center for Number Theory Research at Macquarie University in Sydney; I would like the thank them for their hospitality.

2. Background

In this section we recall various definitions and constructions that will be used in the paper. The reader who wishes to get quickly to the heart of the matter should skim this section and proceed to Sect. 3.

2.1. Differentials

We set the following notation:

R	a complete discrete valuation ring
K	the fraction field of R
$\mathfrak{m}$	the maximal ideal of R
k	the residue field of R
X	a complete nonsingular curve over K, of genus $g > 0$
O	a K-rational point on X
$\mathcal{X}$	the minimal regular model for X over R
$\tilde{\mathcal{X}}$	the special fiber of $\mathcal{X}$
A	the Jacobian of X
$\mathcal{A}$	the Néron model of A
$\tilde{\mathcal{A}}$	the special fiber of $\mathcal{A}$
$\mathcal{A}^0$	the open subscheme of $\mathcal{A}$ whose special fiber is the connected component of $\tilde{\mathcal{A}}$, and whose generic fiber is A
$\Omega^1_{Z/S}$	the sheaf of relative differential forms of degree 1 for a morphism of schemes $Z \to S$
$\omega_{Z/S}$	the relative dualizing sheaf for a morphism $Z \to S$ (when it exists)

The principal reference for the relative dualizing sheaf is [H]. For a condensed guide to the relevant portions of this reference, see [M2], §3. The principal reference for Néron models is [BLR]. Let $T_e(A)$ be the tangent space of A at the identity, and let $T'_e(A) = \mathrm{Hom}_K(T_e(A), K)$ be the cotangent space. Then there is an isomorphism

$$\tau : T'_e(A) \to H^0(X, \Omega^1_{A/K})$$

which takes a cotangent vector v to the unique translation invariant differential whose value at e is v. Let

$$j : X \to A$$

be the embedding that takes $P \in X$ to the point in A represented by the divisor $P - O$. Then pullback by j induces an isomorphism

$$j^* : H^0(A, \Omega^1_{A/K}) \simeq H^0(X, \Omega^1_{X/K}).$$

The K-vector spaces $T'_e(A)$, $H^0(A, \Omega^1_{A/K})$, and $H^0(X, \Omega^1_{X/K})$ all contain natural lattices coming from the models $\mathcal{A}$ and $\mathcal{X}$, and we will need to know that these lattices are preserved under the maps j^* and τ. By a lattice we mean an R-submodule which generates the space over K.

We have a lattice $T'_e(\mathcal{A})$ in $T'_e(A)$ consisting of those tangent vectors which extend to sections of the conormal bundle to the identity section in $\mathcal{A}$. Note that the conormal bundle is just the restriction to the identity section of the sheaf $\Omega^1_{\mathcal{A}/R}$.

Also, since $\mathcal{A}$ is smooth over R, $\Omega^1_{\mathcal{A}/R}$ is a line bundle ([BLR], 4.2, Corollary 3), and restriction to the generic fiber embeds $H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/R})$ as a lattice in $H^0(A, \Omega^1_{A/K})$.

Proposition 1 ([BLR], 4.2, Proposition 2). *We have*

$$\tau(T'_e(\mathcal{A})) = H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/R}).$$

Next, we have the free R-module $H^0(\mathcal{X}, \omega_{\mathcal{X}/R})$ and a canonical isomorphism

$$H^0(\mathcal{X}, \omega_{\mathcal{X}/R}) \otimes_R K \simeq H^0(X, \Omega^1_{X/K}),$$

which identifies $H^0(\mathcal{X}, \omega_{\mathcal{X}/R})$ with a lattice in $H^0(X, \Omega^1_{X/K})$. The isomorphism is explained in [M2], Lemma 3.6, taking account of the fact that $\Omega^1_{X/K}$ is the relative dualizing sheaf for X/K ([M2], Theorem 3.5).

Proposition 2. *We have*

$$j^* H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/R}) = H^0(\mathcal{X}, \omega_{\mathcal{X}/R}).$$

Proof. From [Mi3], Proposition 2.2, we have the following commutative diagram

$$\begin{array}{ccc} H^0(A, \Omega^1_{A/K}) & \xrightarrow{j^*} & H^0(X, \Omega^1_{X/K}) \\ {\scriptstyle \tau^{-1}}\downarrow & & \uparrow{\scriptstyle g} \\ T'_e(A) & \xrightarrow{f} & \mathrm{Hom}_K(H^1(X, \mathcal{O}_X), K), \end{array}$$

where g is the isomorphism derived from Serre duality, and f is the dual of the canonical isomorphism ([Mi3], Proposition 2.1)

$$T_e(A) \simeq H^1(X, \mathcal{O}_X)$$

which comes from the fact $A = \mathrm{Pic}^0_{X/K}$.

We have already seen that $\tau^{-1}(H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/R})) = T'_e(\mathcal{A})$. Further, since $\mathcal{A}^0 = \mathrm{Pic}^0_{\mathcal{X}/R}$ ([BLR], 9.5, Theorem 4), the same argument as in [Mi3], Proposition 2.1 (with K replaced by R) yields a canonical isomorphism

$$T_e(\mathcal{A}) \simeq H^1(\mathcal{X}, \mathcal{O}_{\mathcal{X}}),$$

and hence

$$f(T'_e(\mathcal{A})) = \mathrm{Hom}(H^1(\mathcal{X}, \mathcal{O}_{\mathcal{X}}), R).$$

Finally, duality yields

$$g(\mathrm{Hom}(H^1(\mathcal{X}, \mathcal{O}_{\mathcal{X}}), R)) = H^0(\mathcal{X}, \omega_{\mathcal{X}/R}).$$

Proposition 3. *Restriction to the special fiber induces isomorphisms*

$$H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/R})/\mathfrak{m}H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/R}) \to H^0(\tilde{\mathcal{A}}^0, \Omega^1_{\tilde{\mathcal{A}}^0/k})$$
$$H^0(\mathcal{X}, \omega_{\mathcal{X}/R})/\mathfrak{m}H^0(\mathcal{X}, \omega_{\mathcal{X}/R}) \to H^0(\tilde{\mathcal{X}}, \omega_{\tilde{\mathcal{X}}/k}).$$

Proof. For $\omega_{\mathcal{X}/R}$, this was shown in [M2], Lemma 3.6. For $\Omega^1_{\mathcal{A}/R}$, use the isomorphism from Proposition 1

$$\tau\colon T'_e(\mathcal{A}) \simeq H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/R}),$$

and the canonical isomorphisms

$$H^0(\tilde{\mathcal{A}}^0, \Omega^1_{\tilde{\mathcal{A}}^0/R}) \simeq T'_e(\tilde{\mathcal{A}})$$

and

$$T'_e(\mathcal{A})/\mathfrak{m}T'_e(\mathcal{A}) \simeq T'_e(\tilde{\mathcal{A}}).$$

We denote the reduction of a differential ω by $\tilde{\omega}$. In the case we consider below, $\tilde{\mathcal{X}}$ is reduced, and we therefore have a canonical isomorphism ([M2], Theorem 3.5)

$$\omega_{\tilde{\mathcal{X}}/k} \simeq \Omega^{\mathrm{reg}}_{\tilde{\mathcal{X}}/k},$$

where $\Omega^{\mathrm{reg}}_{\tilde{\mathcal{X}}/k}$ is the sheaf of regular differentials ([S1]).

2.2. *Integrals*

We briefly recall Coleman's theory of p-adic integration. The standard reference for the theory of affinoids and rigid analysis is [BGR]. We denote by $\mathbb{C}_p$ the completion of the algebraic closure of $\mathbb{Q}_p$. Let V be a complete variety over $\mathbb{C}_p$ with good reduction (i.e., which has a smooth proper model over the ring of integers in $\mathbb{C}_p$), and let $\omega \in H^0(V, \Omega^1_{V/\mathbb{C}_p})$. If ω is closed, it is easy to find a locally analytic function λ on the analytic space $V(\mathbb{C}_p)$ such that $d\lambda = \omega$; however, such a λ is not very rigid, since it can be modified by any locally constant function. Using rigid analysis and Dwork's principle of analytic continuation by Frobenius, Coleman showed [C1] how to fix the choice of λ. Coleman's integrals are defined initially on affinoids, and then on varieties by means of a patching procedure. Let $\mathbb{X}$ be a smooth, connected affinoid over $\mathbb{C}_p$ with good reduction (we use the definition of reduction in [C1], Part I). We denote by $A(\mathbb{X})$ the algebra of rigid analytic functions on $\mathbb{X}$, and by $\Omega^1_{\mathbb{X}/\mathbb{C}_P}$ the $A(\mathbb{X})$-module of rigid analytic differentials on $\mathbb{X}$ (see [C1], Part I, §3). For each $\omega \in \Omega^1_{\mathbb{X}/\mathbb{C}_P}$ Coleman constructs integrals

$$\int_P^Q \omega, \quad P, Q \in \mathbb{X}(\mathbb{C}_p),$$

with the following properties.

First, the integral satisfies all the usual properties: it is linear in the integrand, and

$$\int_P^Q \omega = -\int_Q^P \omega$$
$$\int_P^Q \omega = \int_P^O \omega + \int_O^Q \omega.$$

Second, for fixed P, $\lambda(Q) = \int_P^Q \omega$ is a locally analytic function on $\mathbb{X}(\mathbb{C}_p)$ such that $d\lambda = \omega$.

Third, if $f: \mathbb{X} \to \mathbb{Y}$ is a morphism of smooth, connected affinoids with good reduction, then

$$\int_P^Q f^*\omega = \int_{f(P)}^{f(Q)} \omega. \tag{4}$$

Fourth, if σ is a continuous automorphism of $\mathbb{C}_p$ then

$$\left(\int_P^Q \omega\right)^\sigma = \int_{P^\sigma}^{Q^\sigma} \omega^\sigma,$$

where the second integral is taken on $\mathbb{X}^\sigma$.

Finally, if $\omega = df$, $f \in A(\mathbb{X})$, then

$$\int_P^Q \omega = f(Q) - f(P).$$

Patching together these integrals yields integrals on $V(\mathbb{C}_p)$ satisfying the same properties.

2.3. *Logarithms*

The general reference for this section is [B], Sect. 7.6. Let A be an abelian variety over K of dimension d, and let $\mathcal{A}$ be its Néron model over R. If $\omega \in H^0(A, \Omega^1_{A/K})$, then ω is a closed, translation invariant 1-form, and

$$\lambda_\omega(P) = \int_O^P \omega, \quad P \in A(\mathbb{C}_p),$$

is a homomorphism to $\mathbb{C}_p$. The homomorphism

$$A(\mathbb{C}_p) \to T_e(A_{\mathbb{C}_p}) = \mathrm{Hom}_{\mathbb{C}_p}(H^0(A_{\mathbb{C}_p}\Omega^1_{A/\mathbb{C}_p}), \mathbb{C}_p)$$
$$x \mapsto (\omega \mapsto \lambda_\omega(x))$$

is the logarithm map for $A(\mathbb{C}_p)$ as a p-adic Lie group ([B], Sect. 7.6).

Let $\mathcal{A}_1(R)$ be the kernel of the reduction map

$$\mathcal{A}(R) \to \tilde{\mathcal{A}}(k).$$

Then, as a p-adic Lie group, $\mathcal{A}_1(R)$ is isomorphic to $(\mathfrak{m})^d = \mathfrak{m} \times \cdots \times \mathfrak{m}$ with a formal group law on it. Define $\mathcal{A}_n(R)$ to be the subgroup corresponding under this isomorphism to $\mathfrak{m}^n \times \cdots \times \mathfrak{m}^n$ (it is independent of the choice of isomorphism). Let v be the valuation of R such that $v(p) = 1$. By the valuation of an ideal in R we mean the valuation of a generator for the ideal.

Lemma 1. *Suppose* $v(\mathfrak{m}^n) > 1/(p-1)$. *Then* Λ *induces an isomorphism*

$$\Lambda\colon \mathcal{A}_n(R) \to \mathfrak{m}^n T_e(\mathcal{A}).$$

Proof. This follows from [B], 7.6, Proposition 14.

3. Bounding the local dimension

We set the following notation

p	a prime number ≥ 5
A	the Jacobian of $F_{a,b,c}$
ζ	a fixed primitive p^{th} root of unity
K	$\mathbb{Q}(\zeta)$
π	$1-\zeta$
$\mathfrak{p}$	the prime of K above p
$K_\mathfrak{p}$	the completion of K with respect to the $\mathfrak{p}$-adic metric on K
$\mathcal{O}_\mathfrak{p}$	the ring of integers in $K_\mathfrak{p}$
U_k	the image of $1+\pi^k\mathcal{O}_\mathfrak{p}$ in $K_\mathfrak{p}/K_\mathfrak{p}^{*p}$
$A[\pi^n]$	the kernel of π^n on A
$A[\pi^\infty]$	the union of all the $A[\pi^n]$
Δ	$\mathrm{Gal}(K/\mathbb{Q})$
ω	the character $\Delta \to \mathbb{Z}_p^*$ characterized by $\zeta^\sigma = \zeta^{\omega(\sigma)}$

We will regard $A(\mathbb{Q}_p)$ a compact Lie group; its dimension is the genus $g = (p-1)/2$ of $F_{a,b,c}$. The closure $\overline{A(\mathbb{Q})}$ of $A(\mathbb{Q})$ in $A(\mathbb{Q}_p)$ is a Lie subgroup, and our goal in this section is to show that its dimension is strictly less than the dimension of $A(\mathbb{Q}_p)$, subject to the existence of certain cocycles $d_n \in H^1(K, A)$.

If R is an integral domain, M an R-module, and $N \subset M$ is a submodule, we define the *saturation* of N in M to be

$$\{m \in M : rm \in N \text{ for some } r \in R, r \neq 0\}.$$

We say that N is saturated in M if it is equal to its saturation.

Lemma 2. *The saturation of* N *contains the torsion submodule of* M. *If* N *is saturated in* M *and if* $r \in R$, *then*

$$N/rN \to M/rM \quad \textit{is injective.}$$

Proof. Clear from the definitions.

Let $\overline{A(\mathbb{Q})}^{\text{sat}}$ be the saturation of $\overline{A(\mathbb{Q})}$ in $A(\mathbb{Q}_p)$, with respect to their structure as $\mathbb{Z}$-modules. Then $\overline{A(\mathbb{Q})}^{\text{sat}}$ is a Lie subgroup of $A(\mathbb{Q}_p)$.

Lemma 3. *As Lie groups,* $\overline{A(\mathbb{Q})}$ *and* $\overline{A(\mathbb{Q})}^{sat}$ *have the same dimension.*

Proof. The quotient $\overline{A(\mathbb{Q})}^{\text{sat}}/\overline{A(\mathbb{Q})}$ is torsion. A Lie group of dimension d has a neighbourhood of the origin isomorphic to $p\mathbb{Z}_p^d$ [B], 7.6; hence a torsion Lie group has dimension zero.

By Lemma 2, we have a natural injective map of $\mathbb{F}_p$-vector spaces

$$f\colon \overline{A(\mathbb{Q})}^{\mathrm{sat}}/p\overline{A(\mathbb{Q})}^{\mathrm{sat}} \hookrightarrow A(\mathbb{Q}_p)/pA(\mathbb{Q}_p).$$

Proposition 4. *The dimension over $\mathbb{F}_p$ of the cokernel of f is equal to the codimension of $\overline{A(\mathbb{Q})}^{sat}$ as a Lie subgroup of $A(\mathbb{Q}_p)$.*

Proof. Since f is injective, the dimension of the cokernel is

$$\dim_{\mathbb{F}_p} A(\mathbb{Q}_p)/pA(\mathbb{Q}_p) - \dim_{\mathbb{F}_p} \overline{A(\mathbb{Q})}^{\mathrm{sat}}/p\overline{A(\mathbb{Q})}^{\mathrm{sat}}.$$

For any compact Lie group G over $\mathbb{Q}_p$ we have the formula

$$\dim_{\mathbb{F}_p} G/pG - \dim_{\mathbb{F}_p} G[p] = \dim G,$$

where $G[p]$ is the kernel of multiplication by p. This may be seen by choosing a neighbourhood U of the origin such that $U \simeq p\mathbb{Z}_p^d$, where $d = \dim G$, and taking the kernel-cokernel exact sequence of

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U & \longrightarrow & G & \longrightarrow & \Phi & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p} & & \\ 0 & \longrightarrow & U & \longrightarrow & G & \longrightarrow & \Phi & \longrightarrow & 0. \end{array}$$

(Note that Φ is finite since G is compact; hence $\#(\Phi/p\Phi) = \#(\Phi[p])$.) By Lemma 2, $\overline{A(\mathbb{Q})}^{\mathrm{sat}}[p] = A(\mathbb{Q}_p)[p]$; hence

$$\dim_{\mathbb{F}_p} A(\mathbb{Q}_p)/pA(\mathbb{Q}_p) - \dim_{\mathbb{F}_p} \overline{A(\mathbb{Q})}^{\mathrm{sat}}/p\overline{A(\mathbb{Q})}^{\mathrm{sat}} = \dim_{\mathbb{Q}_p} A(\mathbb{Q}_p) - \dim_{\mathbb{Q}_p} \overline{A(\mathbb{Q})}^{\mathrm{sat}},$$

as required.

Corollary 1. *The dimension of $\overline{A(\mathbb{Q})}^{sat}$ is equal to the dimension of $A(\mathbb{Q}_p)$ if and only if f is surjective.*

Let $\chi\colon A(\mathbb{Q}_p)/pA(\mathbb{Q}_p) \to A(K_\mathfrak{p})/\pi A(K_\mathfrak{p})$ be the natural map induced by the inclusion of $A(\mathbb{Q}_p)$ in $A(K_\mathfrak{p})$, and consider the sequence

$$\overline{A(\mathbb{Q})}^{\mathrm{sat}}/p\overline{A(\mathbb{Q})}^{\mathrm{sat}} \xrightarrow{f} A(\mathbb{Q}_p)/pA(\mathbb{Q}_p) \xrightarrow{\chi} A(K_\mathfrak{p})/\pi A(K_\mathfrak{p}). \tag{5}$$

To show that f is not surjective, we will show that χ is non-zero, but that the composite map $\chi \circ f$ is zero. To show the first, we need to do a local π-descent.

Let

$$\delta\colon A(K_\mathfrak{p}) \to H^1(K_\mathfrak{p}, A[\pi])$$

be the coboundary map for cohomology of the sequence

$$0 \to A[\pi] \to A \xrightarrow{\pi} A \to 0.$$

Lemma 4. *The $\mathbb{Q}$-rational divisor $(0,0) - \infty$ on $F_{a,b,c}$ generates $A[\pi]$.*

Proof. See [M2] or do as an exercise.

To describe the image of δ, we will follow [M2] and choose an isomorphism of trivial $\mathrm{Gal}(\overline{K}/K)$-modules

$$\iota\colon A[\pi] \simeq \mu_p.$$

This induces

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

Let δ' be the composite map

$$\delta' = \iota_* \circ \delta\colon A(K_\mathfrak{p}) \to K_\mathfrak{p}^*/K_\mathfrak{p}^{*p}.$$

Lemma 5. *The map δ' is Δ-equivariant.*

Proof. By Lemma 4 $A[\pi]$ is fixed by Δ, and hence $\iota \circ \sigma = \omega^{-1}(\sigma)\sigma \circ \iota$, for $\sigma \in \Delta$. Hence

$$\iota_*(x^\sigma) = \omega^{-1}(\sigma)(\iota_*(x)^\sigma), \quad x \in H^1(K_\mathfrak{p}, A[\pi]). \tag{6}$$

On the other hand, we claim that

$$\delta(P^\sigma) = \omega(\sigma)(\delta(P))^\sigma. \tag{7}$$

Indeed, if $\pi Q = P$, then $\delta(P)$ is represented by the cocycle

$$\tau \mapsto Q^\tau - Q, \quad \tau \in \mathrm{Gal}(\overline{K}/K).$$

Since $(\pi^\sigma/\pi) \equiv \omega(\sigma)$ modulo π, we have $\pi\omega(\sigma)Q^\sigma \equiv P^\sigma$ modulo $\pi A(K_\mathfrak{p})$. Hence $\delta(P^\sigma)$ is represented by the cocycle

$$\tau \mapsto (\omega(\sigma)Q^\sigma)^\tau - (\omega(\sigma)Q^\sigma), \quad \tau \in \mathrm{Gal}(\overline{K}/K),$$

and the claim follows. The lemma now follows from Eqs. (6) and (7).

Recall that U_k is defined to be the image of $1 + \pi^k\mathcal{O}_\mathfrak{p}$ in $K_\mathfrak{p}/K_\mathfrak{p}^{*p}$.

Theorem 2 (Faddeev [F]). *We have*

$$U_{(p+1)/2} \subset \delta'(A(K_\mathfrak{p})) \subset U_{(p-1)/2}.$$

(This also follows from (5.3), (5.6), and Lemma 5.5 of [M2].)

Corollary 2. *The map δ' restricts to an isomorphism*

$$(A(K_\mathfrak{p})/\pi A(K_\mathfrak{p}))^\Delta \simeq \langle 1 + p\rangle \subset K_\mathfrak{p}^*/K_\mathfrak{p}^{*p}.$$

Proof. Since δ' is a Δ-equivariant isomorphism between $A(K_\mathfrak{p})/\pi A(K_\mathfrak{p})$ and $\mathrm{im}\,\delta' \subset K_\mathfrak{p}^*/K_\mathfrak{p}^{*p}$, it suffices to show that $(\mathrm{im}\,\delta')^\Delta$ is generated by $1 + p$. First, since δ' is Δ-equivariant, it follows that $(\mathrm{im}\,\delta')^\Delta \subset (K_\mathfrak{p}^*/K_\mathfrak{p}^{*p})^\Delta \simeq \mathbb{Q}_p^*/\mathbb{Q}_p^{*p}$, where the latter isomorphism follows from the fact that Δ has order prime to p. Now, $\mathbb{Q}_p^*/\mathbb{Q}_p^{*p}$ is generated by p and $1+p$. Since $p \notin U_1$, and $1+p \in U_{p-1}$, and since $p \geq 5$, it follows from Faddeev's theorem that $\mathbb{Q}_p^*/\mathbb{Q}_p^{*p} \cap \mathrm{im}\,\delta'$ is generated by $1 + p$.

Proposition 5. *The map*

$$A(\mathbb{Q}_p)/pA(\mathbb{Q}_p) \xrightarrow{\chi} A(K_\mathfrak{p})/\pi A(K_\mathfrak{p})$$

is non-zero.

Proof. Choose an element $P \in A(K_\mathfrak{p})$ whose class $[P]$ in $A(K_\mathfrak{p})/\pi A(K_\mathfrak{p})$ generates $(A(K_\mathfrak{p})/\pi A(K_\mathfrak{p}))^\Delta$. We can assume $[P] \neq 0$ by Corollary 2. Let

$$Q = \sum_{\sigma \in \Delta} P^\sigma.$$

Then $Q \in A(\mathbb{Q}_p)$, and

$$[Q] = (p-1)[P] = -[P].$$

Hence $\chi(Q) \neq 0$.

Next we want to show that the composite $\chi \circ f$ in the sequence (5) is zero. This will require a global argument.

For each valuation v of K, we have the Tate local pairing [Mi2]

$$\langle\ ,\ \rangle_v \colon A(K_v) \times H^1(K_v, A) \to \mathbb{Q}/\mathbb{Z},$$

which induces a perfect pairing of finite groups

$$\langle\ ,\ \rangle_v \colon A(K_v)/\pi A(K_v) \times H^1(K_v, A)[\pi] \to \mathbb{Q}/\mathbb{Z}.$$

(Note that the dual endomorphism to $\pi = 1 - \zeta$ is $\hat{\pi} = 1 - \zeta^{-1}$, which is a unit times π, so π-torsion and $\hat{\pi}$-torsion are the same.)

The key to bounding the local rank is the existence of elements

$$d_n \in H^1(K, A)[\pi^{n+1}]$$

such that

(H1) $$d_{n,v} = 0 \quad \text{if} \quad v(p) = 0,$$

and

(H2) $\pi_*^n d_{n+1,\mathfrak{p}}$ pairs non-trivially with $(A(K_\mathfrak{p})/\pi A(K_\mathfrak{p}))^\Delta$.

In Sect. 5 we will show how to construct d_n in the case that p is regular. For now, we will assume the existence of d_n and show how to derive the Second Case.

Theorem 3. *Suppose that for each $n \geq 0$ there exists $d_n \in H^1(K, A)$ satisfying (H1) and (H2). Then the saturation $\overline{A(\mathbb{Q})}^{sat}$ of $\overline{A(\mathbb{Q})}$ in $A(\mathbb{Q}_p)$ is contained in $\pi A(K_\mathfrak{p})$.*

Proof. Let P be an element of $\overline{A(\mathbb{Q})}^{\text{sat}}$. Then there exists $Q \in \overline{A(\mathbb{Q})}$ and $r \in \mathbb{Z}$ such that

$$rP = Q.$$

Let $n = \text{ord}_\pi(r)$. For any $S \in A(K)$, we have

$$\sum_v \langle S, d_n \rangle_v = 0$$

because the sum of the invariants of an element of the global Brauer group is zero. Hence it follows from (H1) that

$$\langle S, d_n \rangle_{\mathfrak{p}} = 0.$$

If we choose S sufficiently close to Q, we may deduce that

$$\langle Q, d_n \rangle_{\mathfrak{p}} = 0.$$

Now write

$$r = \pi^n u, \quad u \in \mathcal{O}_{\mathfrak{p}}{}^*.$$

Then

$$0 = \langle Q, d_n \rangle_{\mathfrak{p}} = \langle rP, d_n \rangle_{\mathfrak{p}} = \langle uP, \hat{\pi}_*^n d_n \rangle_{\mathfrak{p}},$$

where $\hat{\pi}$ is the dual endomorphism to π. Now, P is fixed by Δ and u is congruent to a rational integer modulo π; hence the image of uP in $A(K_{\mathfrak{p}})/\pi A(K_{\mathfrak{p}})$ is fixed by Δ. Since $\hat{\pi}$ is a unit times π, it follows from (H2) that $P \in \pi A(K_{\mathfrak{p}})$ as required.

Corollary 3. *With the hypothesis in Theorem 3, the dimension of* $\overline{A(\mathbb{Q})}$ *is less than the dimension of* $A(\mathbb{Q}_p)$.

Proof. A reformulation of the theorem is that the composite map $\chi \circ f$ in the sequence (5) is zero. On the other hand, from Lemma 5, we know that χ is not zero. Hence f is not surjective. The corollary now follows from Corollary 1.

4. Bounding the rational points

We defer certain calculations having to do with the specific nature of the curve $F_{a,b,c}$. We need, however, a piece of terminology relating to the fiber type of the minimal regular model. We say that $F_{a,b,c}$ is *tame* if

$$\frac{(a^a b^b c^c)^p - a^a b^b c^c}{p} \equiv 0 \pmod{p},$$

and is *wild* if

$$\frac{(a^a b^b c^c)^p - a^a b^b c^c}{p} \not\equiv 0 \pmod{p},$$

The relation between these conditions and the minimal regular model is explained in [M1].

We assume throughout this section that $F_{a,b,c}$ is wild. Let $X = A$ or $X = F_{a,b,c}$. If $\omega \in H^0(X, \Omega^1_{X/\mathbb{Q}_p})$ is a closed holomorphic differential on X, we let

$$\lambda_\omega(P) = \int_O^P \omega, \quad P \in X(\mathbb{C}_p),$$

where the base point O is the identity e in the case $X = A$, and the point $(0,0)$ in the case $X = F_{a,b,c}$, and the integral is the p-adic integral defined by Coleman and recalled in Sect. 2.2.

We have a pairing

$$\begin{aligned} A(\mathbb{Q}_p) \times H^0(A, \Omega^1_{A/\mathbb{Q}_p}) &\to \mathbb{Q}_p \\ (x, \omega) &\mapsto \lambda_\omega(x). \end{aligned} \tag{8}$$

Lemma 6. *The pairing (8) is non-degenerate on the right and its kernel on the left is* $A(\mathbb{Q}_p)_{tor}$.

Proof. As explained in Sect. 2.3, the corresponding map

$$\Lambda\colon A(\mathbb{Q}_p) \to \mathrm{Hom}(H^0(A, \Omega^1_{A/\mathbb{Q}_p}), \mathbb{Q}_p) = T_e(A)$$

is the logarithm map for $A(\mathbb{Q}_p)$. The lemma now follows from the fact that the kernel of the logarithm is $A(\mathbb{Q}_p)_{\mathrm{tor}}$ [B], Sect. 7.6, Proposition 12.

Now, $A(\mathbb{Q}_p)/A(\mathbb{Q}_p)_{\mathrm{tor}}$ is a torsion-free $\mathbb{Z}_p$-module of rank g, and hence is free. It follows from Corollary 3 that the image of $\overline{A(\mathbb{Q})}^{\mathrm{sat}}$ in $A(\mathbb{Q}_p)/A(\mathbb{Q}_p)_{\mathrm{tor}}$ is a submodule of rank less than g. Further, the image of $\overline{A(\mathbb{Q})}^{\mathrm{sat}}$ in $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ is contained in the kernel of χ. Choose once and for all a saturated submodule $M \subset A(\mathbb{Q}_p)$, such that

- $\overline{A(\mathbb{Q})}^{\mathrm{sat}} \subset M$,
- $M/A(\mathbb{Q}_p)_{\mathrm{tor}}$ is a free rank $g-1$ $\mathbb{Z}_p$-module, and
- the image of M in $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ is the kernel of χ.

Then under the pairing (8), the annihilator of M is a one-dimensional saturated submodule N of $H^0(A, \Omega^1_{A/K})$. Recall that $j\colon F_{a,b,c} \hookrightarrow A$ is the embedding that takes $(0,0)$ to e.

Proposition 6. *Let* $\omega \in H^0(F_{a,b,c}, \Omega^1_{F_{a,b,c}/\mathbb{Q}_p})$ *be defined by* $\omega = j^*\eta$, *where* $\eta \in H^0(A, \Omega^1_{A/K})$ *is a generator of* N. *Then* $\omega \neq 0$ *and* $\lambda_\omega(P) = 0$ *for all* $P \in F_{a,b,c}(\mathbb{Q})$.

Proof. Let η be as above. If $x \in A(\mathbb{C}_p)$ is represented by the divisor D of degree zero on $F_{a,b,c}$, then, since λ_η is a homomorphism, we have

$$\lambda_\eta(x) = \sum_{P \in F_{a,b,c}} \mathrm{ord}_P(D)\lambda_\eta(j(P)).$$

It follows from Eq. (4) that

$$\sum_{P \in F_{a,b,c}} \mathrm{ord}_P(D)\lambda_\eta(j(P)) = \sum_{P \in F_{a,b,c}} \mathrm{ord}_P(D)\lambda_\omega(P).$$

Now, from the definition of η we have $\lambda_\eta(x) = 0$ for all $x \in \overline{A(\mathbb{Q})}^{\text{sat}}$, hence *a fortiori* $\lambda_\eta(x) = 0$ for all $x \in A(\mathbb{Q})$. Thus, if D is rational over $\mathbb{Q}$,

$$\sum_{P \in F_{a,b,c}} \operatorname{ord}_P(D)\lambda_\omega(P) = 0.$$

Now $\lambda_\omega((0,0)) = 0$, since $j((0,0)) = e$; hence, if $P \in F_{a,b,c}(\mathbb{Q})$, we have

$$\lambda_\omega(P) = \lambda_\omega(P) - \lambda_\omega(0,0) = 0.$$

The proposition already implies that $F_{a,b,c}$ has at most $2p-3$ $\mathbb{Q}$-rational points, as explained in [M3]. To do better than that we will pin down ω more precisely by using Theorem 3 rather than Corollary 3. The idea is to take advantage of the fact that we know the image of M in $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ in order to determine ω mod p. In fact, since all we know about M explicitly is its image $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p$, that's all we can use. First we need a version of the pairing (8) that takes account of the $\mathbb{Z}_p$-structure on the right hand side.

Proposition 7. *The pairing (8) induces a pairing*

$$A(\mathbb{Q}_p) \times H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/\mathbf{Z}_p}) \to \mathbb{Z}_p. \tag{9}$$

Proof. From Lemma 1 we know (since $p > 2$) that Λ induces an isomorphism

$$\Lambda\colon \mathcal{A}_1(\mathbb{Z}_p) \simeq pT_e(\mathcal{A}). \tag{10}$$

Now

$$A(\mathbb{Q}_p)/\mathcal{A}_1(\mathbb{Z}_p) \simeq \tilde{A}(\mathbb{F}_p) \simeq \mathbb{F}_p^g,$$

the last isomorphism following from Lemma 11. In particular, $A(\mathbb{Q}_p)/\mathcal{A}_1(\mathbb{Z}_p)$ is killed by p; hence

$$\Lambda(A(\mathbb{Q}_p)) \subset T_e(\mathcal{A}) = \operatorname{Hom}(T'_e(\mathcal{A}), \mathbb{Z}_p) = \operatorname{Hom}(H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/\mathbf{Z}_p}), \mathbb{Z}_p).$$

The proposition follows.

By Proposition 3, and the fact that $\tilde{\mathcal{A}}$ is connected, we have

$$H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/\mathbf{Z}_p})/\mathfrak{m}H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/\mathbf{Z}_p}) \simeq H^0(\tilde{\mathcal{A}}, \Omega^1_{\tilde{\mathcal{A}}/\mathbb{F}_p}).$$

Hence, the pairing (9) induces a pairing

$$A(\mathbb{Q}_p)/pA(\mathbb{Q}_p) \times H^0(\tilde{\mathcal{A}}, \Omega^1_{\tilde{\mathcal{A}}/\mathbf{F}_p}) \to \mathbb{F}_p. \tag{11}$$

Let $W \subset H^0(\tilde{\mathcal{A}}, \Omega^1_{\tilde{\mathcal{A}}/\mathbf{F}_p})$ be the annihilator of $\ker\chi$ under the pairing (11). If $F_{a,b,c}$ is wild, then, as we shall show in Proposition 8, the naive model for $F_{a,b,c}$ obtained by taking the normalization of the projective completion of the affine curve over $\mathbb{Z}$ defined by Eq. (2) is the minimal regular model $\mathcal{F}^{\text{reg}}_{a,b,c}$. This model has a cusp at the point ξ where

$$\tilde{x}(\xi) = \frac{-\tilde{a}}{\tilde{c}},$$

and is otherwise non-singular. Denote the points $(0,0),(1,0)$, and ∞ on $F_{a,b,c}$ by A, B, and C respectively. By Proposition 2, we have an isomorphism

$$j^*: H^0(\mathcal{A}, \Omega^1_{\mathcal{A}/\mathbf{Z}_p}) \simeq \mathcal{H}^1(\mathcal{F}^{\mathrm{reg}}_{a,b,c}, \omega_{\mathcal{F}^{\mathrm{reg}}_{a,b,c}/\mathbf{Z}_p}).$$

In view of Proposition 3, this induces an isomorphism

$$\tilde{j}^*: H^0(\tilde{\mathcal{A}}, \Omega^1_{\tilde{\mathcal{A}}/\mathbf{F}_p}) \simeq H^0(\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}, \omega_{\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}/\mathbf{F}_p}).$$

Let $V = \tilde{j}^* W$. The calculation of V is the key to bounding the rational points. We will defer that calculation to Sect. 8; here we will report the results of that calculation and show how to use them to prove the main theorem.

Theorem 4. *Suppose $F_{a,b,c}$ is wild. Then*

$$V \cap H^0(\tilde{\mathcal{F}}^{reg}_{a,b,c}, \omega_{\tilde{\mathcal{F}}^{reg}_{a,b,c}/\mathbf{F}_p}(-\tilde{A} - \tilde{B} - \tilde{C})) = 0.$$

If $P \in \tilde{\mathcal{F}}^{reg}_{a,b,c}(\mathbb{F}) - \{\xi, \tilde{A}, \tilde{B}, \tilde{C}\}$ then

$$V \cap H^0(\tilde{\mathcal{F}}^{reg}_{a,b,c}, \omega_{\tilde{\mathcal{F}}^{reg}_{a,b,c}/\mathbf{F}_p}(-2P)) = 0.$$

We will prove this in Sect. 8. To apply it, we need the following lemma.

Lemma 7. *Let $f \in \mathbb{Q}_p[[T]]$, and suppose that its derivative f' is in $\mathbb{Z}_p[[T]]$. Let i_0 be the order of vanishing of the reduction $\tilde{f}'$ of f' mod p. If $i_0 < p-2$, then f has at most $i_0 + 1$ zeroes in $p\mathbb{Z}_p$.*

Proof. This is a special case of Lemma 3 in [C1]; for the convenience of the reader, we reproduce a proof here. Suppose f has a zero in $p\mathbb{Z}_p$; translating to the origin we may assume that $f(0) = 0$. Let

$$f(T) = \sum_{k=1}^{\infty} \frac{a_k}{k} T^k, \quad a_k \in \mathbb{Z}_p.$$

Let

$$g(T) = f(pT) = \sum_{k=1}^{\infty} \frac{p^k a_k}{k} T^k.$$

Then $g(T)$ has integer coefficients. By hypothesis, $|a_{i_0+1}| = 1$, so

$$\left| \frac{p^{i_0+1} a_{i_0+1}}{i_0+1} \right| = \left| \frac{p^{i_0+1}}{i_0+1} \right|.$$

On the other hand, since $i_0 < p-2$

$$\left| \frac{p^k a_k}{k} \right| \leq \left| \frac{p^k}{k} \right| < \left| \frac{p^{i_0+1}}{i_0+1} \right| \quad k > i_0 + 1.$$

Thus the coefficient with the largest absolute value in $g(T)$ occurs in degree less than or equal to $i_0 + 1$; the lemma now follows from the Weierstrass preparation theorem.

Lemma 8. *The map (3) $F \to F_{a,b,c}$ induces bijections*

$$F(\mathbb{Q}) \simeq F_{a,b,c}(\mathbb{Q})$$

and

$$F(\mathbb{F}_p) \simeq F_{a,b,c}(\mathbb{F}_p).$$

Proof. In terms of the affine equations

$$x^p + y^p = 1$$

and

$$t^p = (-1)^c s^a (1-s)^b$$

the map is given by the equations

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

Since every element of either $\mathbb{Q}$ or $\mathbb{F}_p$ has at most one p-th root, the map is clearly injective on $\mathbb{Q}$- or $\mathbb{F}_p$-rational points. Now suppose $(s,t) \in F_{a,b,c}(K)$, where K is $\mathbb{Q}$ or $\mathbb{F}_p$. Then it follows from the equations that (s,t) is in the image of the map if and only if s and $1-s$ are p-th powers in K. Every element of $\mathbb{F}_p$ is a p-th power. As for $\mathbb{Q}$, we note that since

$$t^p = (-1)^c s^a (1-s)^b,$$

both s and $1-s$ have order divisible by p at each prime $q \in \mathbb{Z}$, as may be easily seen by taking valuations of both sides. Hence they are both p-th powers, as required.

Proof of Theorem 1. In the case $p = 3$ the theorem was proved by Euler [E], without the hypothesis, so we may assume $p > 3$.

Let ω be the differential guaranteed by Proposition 6. We will apply Lemma 7 with $f = \lambda_\omega$. We have $df = \omega$, and, acccording to Theorem 4, $\tilde{\omega}$ does not vanish at one of the points $\tilde{A}$, $\tilde{B}$, and $\tilde{C}$. Hence, by Lemma 7, λ_ω has at most one zero in the residue class of that point. Since λ_ω vanishes at all points of $F_{a,b,c}(\mathbb{Q})$, it has exactly one zero, namely the trivial point in that residue class. Hence, that trivial point is the only one in its residue class. Now the three points A, B, and C are the images of the trivial points $(0,1,1)$, $(1,0,1)$, and $(1,-1,0)$ in $F(\mathbb{Q})$. Hence, by Lemma 8, one of those points is the only $\mathbb{Q}$-rational point in its residue class. But the automorphism $(X,Y,Z) \mapsto (-Y,Z,X)$ of F permutes these three points, so in fact each of them is the only $\mathbb{Q}$-rational point in its residue class. This proves the second case. Similarly, if $\tilde{P} \neq \tilde{A}, \tilde{B}, \tilde{C}$ or ξ, then, by Theorem 4, λ_ω cannot have more than two zeroes in the residue class of $\tilde{P}$, and hence there are no more than two rational points in that residue class. Hence there are no more than two rational points in the corresponding residue class of F. This takes care of all the residue classes on F, with the possible exception of $x \equiv (-a/c)$. By the following lemma, we may vary the choice of (a,b,c), and take care of that one as well.

Lemma 9. *If $p > 3$ there exist at least two triples $(a,b,c) = (s,1,-(s+1))$, $1 \leq s \leq p-2$, such that $F_{a,b,c}$ is wild.*

Proof. We must show that

$$\frac{(a^a b^b c^c)^p - a^a b^b c^c}{p} \not\equiv 0 \pmod{p}$$

for two such triples. We refer to the notation of [M1]. By the remark on page 63 of *op. cit.*, it suffices to show that there are at least two $s \in \mathbb{F}_p$, $s \neq 0, -1$, which are not roots of

$$\phi(x) = \frac{(x+1)^p - x^p - 1}{p}.$$

This follows immediately from the Lemma on page 59 of *op. cit.*, which states that any such root not equal to 0 or -1 must be a double root; hence there can be at most $(p-3)/2$ such roots, leaving $(p-3)/2$ which cannot be roots.

5. The regular case

We conclude this part of the paper with the construction of the cohomology classes d_n in the case that p is regular. We will construct them as the image in $H^1(K, A)$ of certain classes c_n in $H^1(K, A[\pi^n])$. Recall the isomorphism

$$\iota : A[\pi] \simeq \mu_p$$

chosen in Sect. 3, and the corresponding isomorphism

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

Let

$$c_1 = (\iota_*)^{-1}(\zeta).$$

Let d_1 be the image of c_1 in $H^1(K, A)[\pi]$ induced by the inclusion map $A[\pi] \hookrightarrow A$.

Lemma 10. *The Tate pairing between the restriction of d_1 to $H^1(K_\mathfrak{p}, A)$ and $(A(K_\mathfrak{p})/\pi A(K_\mathfrak{p}$ is non-trivial.*

Proof. Consider the exact sequence

$$0 \to A(K_\mathfrak{p})/\pi A(K_\mathfrak{p}) \xrightarrow{\delta} H^1(K_\mathfrak{p}, A[\pi]) \to H^1(K_\mathfrak{p}, A)[\pi] \to 0.$$

If $P \in A(K_\mathfrak{p})/\pi A(K_\mathfrak{p})$, then

$$\langle P, d_1 \rangle = \delta(P) \cup c_1,$$

where the cup product is with respect to the Weil pairing (see [Mi2], I.3.5 and III, Appendix C). Further, under the isomorphism

$$\iota_{*,\mathfrak{p}} : H^1(K_\mathfrak{p}, A[\pi]) \simeq K_\mathfrak{p}^*/K_\mathfrak{p}^{*p}$$

the cup product pairing becomes identified with the Hilbert pairing ([M2], Lemma 2.7), and

$$\langle \iota_*(c_1) \rangle = \langle \zeta \rangle.$$

Let P be a generator of $(A(K_\mathfrak{p})/\pi A(K_\mathfrak{p}))^\Delta$. Then $\iota_*(\delta(P)) = \delta'(P)$. From Corollary 2, it follows that

$$\langle \delta'(P) \rangle = \langle 1 + p \rangle.$$

The lemma now follows from the well known fact that the Hilbert pairing of ζ and $1+p$ is non-trivial (see [CF], Exercises).

Let $U = \text{spec}(\mathcal{O}_K[1/p])$, and let $H^1(U, A[\pi^n])$ be the étale cohomology group of $A[n]$ regarded as an étale sheaf over U. The condition (H1) is equivalent to saying that $d_n \in H^1(U, A)$ ([Mi2], I.3.8). Note that $c_1 \in H^1(U, A[\pi])$, since ζ is a unit.

Theorem 5. *Suppose that p is regular. Then*

$$\pi_* : H^1(U, A[\pi^n]) \longrightarrow H^1(U, A[\pi^{n-1}])$$

is surjective for all n.

Proof. From the cohomology of the exact sequence of étale sheaves over U

$$0 \longrightarrow A[\pi] \longrightarrow A[\pi^n] \xrightarrow{\pi} A[\pi^{n-1}] \longrightarrow 0$$

we see that it suffices to show that

$$H^2(U, A[\pi]) = 0.$$

From the isomorphism

$$\iota\colon A[\pi] \simeq \mu_p$$

and cohomology of the short exact sequence

$$0 \longrightarrow \mu_p \longrightarrow \mathbb{G}_\mathrm{m} \xrightarrow{p} \mathbb{G}_\mathrm{m} \longrightarrow 0$$

we deduce that it suffices to show that both $H^1(U, \mathbb{G}_\mathrm{m})/pH^1(U, \mathbb{G}_\mathrm{m})$ and $H^2(U, \mathbb{G}_\mathrm{m})$ are zero. Now, $H^2(U, \mathbb{G}_\mathrm{m})$ is the subgroup of the Brauer group of K consisting of elements whose invariant at every prime except $\mathfrak{p}$ and the infinite primes is zero, (see [Mi1], III.2.22(f)). Since all the infinite primes are complex, the invariants are zero there also, and since the sum of the invariants must be zero, the invariant at $\mathfrak{p}$ is zero. Hence $H^2(U, \mathbb{G}_\mathrm{m}) = 0$. Finally, since $\mathfrak{p}$ is principal, $\text{Pic}(U) \simeq \text{Pic}(\mathcal{O}_K)$, and since p is regular, $\text{Pic}(\mathcal{O}_K)/p\,\text{Pic}(\mathcal{O}_K) = 0$.

The construction of d_n is now immediate; start with c_1 and lift repeatedly to a $c_n \in H^1(U, A[\pi^n])$ such that $(\pi^{n-1})_* c_n = c_1$, then let d_n be the image of c_n in $H^1(K, A)$ induced by the inclusion map $A_n \hookrightarrow A$.

Remark 1. In fact, one can avoid the need for d_n, $n > 1$, in the regular case, by noticing that $\overline{A(\mathbb{Q})}$ is already saturated in $A(\mathbb{Q}_p)$. If it weren't, there would exist

$$P \in A(\mathbb{Q}) \setminus pA(\mathbb{Q}) \tag{12}$$

such that

$$P \in pA(\mathbb{Q}_p). \tag{13}$$

Let m be the largest integer such that $P \in \pi^m A(K)$. Then by condition (12), $m < p-1$, and hence by condition (13), $P \in \pi^{m+1} A(K_\mathfrak{p})$. Hence $K(\pi^{-(m+1)}P)$ is a non-trivial unramified extension of K of degree p, which contradicts the fact that p is regular. Hence $\overline{A(\mathbb{Q})}$ is saturated in $A(\mathbb{Q}_p)$. It follows that in the proof of Theorem 3 one may take $n = 0$, and hence only d_1 is needed.

6. Models for Fermat curves

In this section we construct various models for Fermat curves. First we construct the minimal regular model for $F_{a,b,c}$ over $\mathbb{Z}_p$, and use it to prove a lemma about the Néron model for A. Then we will construct a smooth model for $F_{a,b,c}$ and use it to prove a lemma about the rigid analytic geometry of $F_{a,b,c}$.

We start with the naive models for F and $F_{a,b,c}$. The naive model for F is the projective scheme $\mathcal{F}$ over $\mathbb{Z}$ defined by the equation

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

The naive model for $F_{a,b,c}$, which we denote by $\mathcal{F}_{a,b,c}$, is the normalization of the projective completion of the affine curve over $\mathbb{Z}$ defined by the equation

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

The special fiber $\tilde{\mathcal{F}}_{a,b,c}$ 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

$$\mathfrak{m}_\xi = (x + \frac{a}{c}, y + a^a b^b c^c, p). \tag{14}$$

(See [M1].)

Recall the classification of $F_{a,b,c}$ into wild and tame: $F_{a,b,c}$ is tame if

$$\frac{(a^a b^b c^c)^p - a^a b^b c^c}{p} \equiv 0 \pmod{p},$$

and is wild if

$$\frac{(a^a b^b c^c)^p - a^a b^b c^c}{p} \not\equiv 0 \pmod{p}.$$

Note that the condition for tameness,

$$\frac{(a^a b^b c^c)^p - a^a b^b c^c}{p} \equiv 0, \pmod{p}$$

is equivalent to $a^a b^b c^c \in \mathbb{Q}_p^{*p}$.

Proposition 8. *If $F_{a,b,c}$ is wild, then $\mathcal{F}_{a,b,c}$ is the minimal regular model for $F_{a,b,c}$. If $F_{a,b,c}$ is tame, then the minimal regular model may be obtained by blowing up ξ once. The exceptional divisor is a non-singular rational curve.*

Proof. First, suppose $F_{a,b,c}$ is wild. Then we claim that ξ is a regular point of $\mathcal{F}_{a,b,c}$. We will eliminate p from the generators of $\mathfrak{m}_\xi$ given in Eq. (14) by showing that

$$p \in \mathfrak{m}_\xi^2.$$

Make the change of coordinates

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

Then

$$\mathfrak{m}_\xi = (s, t, p),$$

and

$$y^p = (a^a b^b c^c)^p (1+t)^p = (a^a b^b c^c)^p (1 + pt + \cdots + t^p),$$
$$(-1)^c x^a (1-x)^b = a^a b^b c^c (1+s)^a (1 - \frac{a}{b} s)^b = a^a b^b c^c (1 + \frac{ac}{2b} s^2 \psi(s)),$$

where $\psi(s) \in \mathbb{Q}[s] \cap \mathbb{Z}_p[s]$. Equating right hand sides and rearranging yields

$$(15) \qquad (a^a b^b c^c)^p - a^a b^b c^c = -(a^a b^b c^c)^p (pt + \cdots + t^p) + a^a b^b c^c (\frac{ac}{2b} s^2 + \cdots).$$

The right hand side is in $\mathfrak{m}_\xi^2$; on the other hand, since $F_{a,b,c}$ is wild, the left hand side is p times a p-adic unit. This proves the claim.

Now, suppose that $F_{a,b,c}$ is tame. As noted above, this means $a^a b^b c^c \in \mathbb{Q}_p^{*p}$. Make the change of coordinates

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

Then

$$y^p = a^a b^b c^c (1+t)^p$$
$$(-1)^c x^a (1-x)^b = a^a b^b c^c (1+s)^a (1 - \frac{a}{b} s)^b = a^a b^b c^c (1 + \frac{ac}{2b} s^2 \psi(s)),$$

hence

$$(16) \qquad (1+t)^p - 1 = \frac{ac}{2b} s^2 \psi(s).$$

As before, ξ is the point with maximal ideal $m_\xi = (x, t, p)$. The scheme defined by this equation is not regular at ξ, but a simple blow-up produces a regular scheme; indeed, if we make the substitution $s = ps'$, $t = pt'$, and divide by p^2, the left hand side acquires a term t', and all other terms are in $\mathfrak{m}_\xi^2$. The special fiber has two components, the exceptional divisor and the proper transform. The proper transform has equation

$$\tilde{t}' = \frac{ac}{2b} \tilde{s}'^2,$$

which is a non-singular rational curve.

Let $\mathcal{A}$ be the Néron model of A over $\mathbb{Z}_p$, and let $\tilde{A}$ be its special fiber.

Lemma 11. *Suppose that $F_{a,b,c}$ is wild. We have*

$$\tilde{A} \simeq \mathbb{G}_a^{(p-1)/2}.$$

Proof. If $F_{a,b,c}$ is wild, then, since $\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}$ is reduced and irreducible, $\tilde{\mathcal{A}}$ is separable and connected. Hence [Ra] there is a canonical isomorphism

$$\tilde{\mathcal{A}} \simeq \mathrm{Pic}^0(\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}).$$

We have from Eq. (15) the equation

$$\tilde{t}^p = \frac{ac}{2b}\tilde{s}^2\psi(\tilde{s}) \tag{17}$$

for $\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}$. Thus $\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}$ has a cusp of order $(p-1)/2$ at ξ, and hence

$$\mathrm{Pic}^0(\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}) \simeq \mathbb{G}_{\mathrm{a}}^{(p-1)/2}, \tag{18}$$

by a standard calculation which we now sketch. Let

$$n\colon \tilde{\mathcal{F}}^{\mathrm{reg,n}}_{a,b,c} \to \tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}$$

be the normalization of $\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}$, and consider the exact sequence

$$0 \to n_*\mathcal{O}^*_{\tilde{\mathcal{F}}^{\mathrm{reg,n}}_{a,b,c}} \to \mathcal{O}_{\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}} \to S \to 0.$$

Here S is a skyscraper sheaf supported at ξ with fiber

$$S_\xi = \mathcal{O}^*_\xi / \mathcal{O}_\xi^{((p-1)/2)*},$$

where $\mathcal{O}_\xi$ is the completion of the local ring $n_*\mathcal{O}_{\tilde{\mathcal{F}}^{\mathrm{reg,n}}_{a,b,c},\xi}$, and $\mathcal{O}_\xi^{((p-1)/2)}$ is the subring generated by s and t, which may be seen, by an explicit uniformization of Eq. (17), to consist of all elements that are constant modulo the $(p-1)/2$-th power of the maximal ideal. (The passage to the completion is justified by [Ma], Theorem 54, p.168.) Since $(p-1)/2 < p$, it follows from [S2], Proposition 9, p. 103, that $S \simeq \mathbb{G}_{\mathrm{a}}(\mathbb{F}_p)^{(p-1)/2}$. Taking cohomology of the exact sequence yields

$$\mathrm{Pic}^0(\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c})(\mathbb{F}_p) \simeq S \simeq \mathbb{G}_{\mathrm{a}}(\mathbb{F}_p)^{(p-1)/2}.$$

The same calculation works over any extension of $\mathbb{F}_p$, hence we have the isomorphism (18), and hence the lemma.

We can now prove the following lemma, which will be used in Sect. 8.

Lemma 12. *If $F_{a,b,c}$ is wild, then the torsion subgroup of $A(\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, and generated by the divisor $(0,0) - \infty$.*

Proof. The divisor of x is $p(0,0) - p\infty$, so the point $P \in A(\mathbb{Q}_p)$ represented by $(0,0) - \infty$ generates a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z}$. In fact, this subgroup is killed by π, since ζ fixes x. Since the degree of π is p, we have $\langle P\rangle = A[\pi](\overline{\mathbb{Q}}_p)$. We want to show that $\langle P\rangle$ is all the torsion. So let Q be a torsion point, not in the subgroup generated by P. By Lemma 1, with $\mathfrak{m} = (p)$ and $n = 1$, the kernel of reduction $A_1(\mathbb{Q}_p)$ is torsion-free, and hence the torsion injects into $\mathbb{F}_p^{(p-1)/2}$. Thus Q is a p-torsion point. Hence, over the ring $\mathbb{Z}[\zeta_p]$, Q has order π^k, $1 \le k \le p-1$. In fact, we must have $k \ge 2$, since $Q \notin \langle P\rangle = A[\pi](\overline{\mathbb{Q}}_p)$. Thus, $\pi^i Q = uP$ for some k, $1 \le i \le p-2$, and some $u \in \mathbb{Z}$. Since

$$\pi^\sigma \equiv \omega(\sigma)\pi \pmod{\pi^2}$$

for $\sigma \in \Delta$, and since Δ fixes Q, this implies that Δ does not fix P; this contradiction proves the Lemma.

Remark. A similar calculation shows that in the tame case the torsion subgroup of $A(\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}/2p\mathbb{Z}$.

We will also need a smooth model for $F_{a,b,c}$. Let ϖ be the unique uniformizer in $K_\mathfrak{p}$ such that

$$\varpi^{p-1} = -p \quad \text{and} \quad \frac{\varpi}{\pi} \equiv 1 \pmod{\mathfrak{p}}.$$

Let

$$L = K_\mathfrak{p}(\varpi^{\frac{1}{2}}, (a^a b^b c^c)^{\frac{1}{p}}).$$

Then over $\mathcal{O}_L$ we get a smooth model $\mathcal{F}^{\mathrm{sm}}_{a,b,c}$ by making the change of coordinates

$$\begin{aligned} x &= \frac{-a}{c}(1 + \varpi^{\frac{p}{2}} u), \\ y &= (a^a b^b c^c)^{\frac{1}{p}}(1 + \varpi v). \end{aligned} \tag{19}$$

The special fiber of $\mathcal{F}^{\mathrm{sm}}_{a,b,c}$ is the Artin-Schreier curve

$$\tilde{v}^p - \tilde{v} = \frac{ac}{2b}\tilde{u}^2. \tag{20}$$

In what follows, we will consider $F_{a,b,c}$ as an object in the rigid analytic category over $\mathbb{C}_p$. For general facts about rigid analysis, we refer the reader to [BGR]. If $F_{a,b,c}$ is wild, let $\mathbb{X}$ be the affinoid in $F_{a,b,c}$ reducing to the nonsingular locus of $\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}$, and if $F_{a,b,c}$ is tame, let $\mathbb{X}$ be the affinoid reducing to the nonsingular locus of the proper transform of $\tilde{\mathcal{F}}_{a,b,c}$ in $\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}$, and, also in the tame case, let $\mathbb{X}'$ be the affinoid reducing to the nonsingular locus of the exceptional divisor. Since in each case $\tilde{\mathbb{X}}$ and $\tilde{\mathbb{X}}'$ are isomorphic to affine lines, each of $\mathbb{X}$ and $\mathbb{X}'$ is isomorphic over $\mathbb{C}_p$ to a closed p-adic disc ([BGR], 6.4.2, Corollary 3, and 3.6, Proposition 12).

Since $F_{a,b,c}$ has positive genus, $\mathbb{X}$ and $\mathbb{X}'$ must be contained in residue classes R and R' of the smooth model of $F_{a,b,c}$ (since otherwise the reduction of the inclusions of these affinoids would induce a non-trivial map from $\mathbb{P}^1$ to the special fiber of the smooth model). It is not hard to see that R is the residue class of the point at infinity on the curve (20), and that R' is the residue class of the point $(0,0)$. For a positive real number r, denote by $\mathbb{B}[r]$ the closed unit ball of radius r, and by $\mathbb{B}(r)$ the open unit ball of radius r, as rigid analytic spaces over $\mathbb{C}_p$ (i.e., $\mathbb{B}[r]$ is the affinoid whose Tate algebra is the subalgebra of $\mathbb{C}_p[[T]]$ consisting of power series with radius of convergence greater than or equal to r, and $\mathbb{B}(r)$ is the union of all $\mathbb{B}[r']$, for $r' < r$).

Lemma 13. *There exists a rigid analytic isomorphism $W\colon R \to \mathbb{B}(1)$ such that*

$$W(\mathbb{X}) = \mathbb{B}[|\varpi^{\frac{1}{2}}|].$$

If $a^a b^b c^c \in \mathbb{Q}_p^{*p}$, there exists an isomorphism $W'\colon R' \to \mathbb{B}(1)$ such that

$$W'(\mathbb{X}') = \mathbb{B}[|\varpi^{\frac{p-2}{2}}|].$$

Proof. First, note that $\mathbb{X}$ is the complement of the residue class of $\mathcal{F}^{\mathrm{reg}}_{a,b,c}$ defined by the inequalities

$$|s| < 1 \text{ and } |t| < 1.$$

Equation (17) tells us that $|t| < 1$ if $|s| < 1$, so $\mathbb{X}$ is defined by the inequality

$$|s| \geq 1.$$

But

$$s = \varpi^{\frac{p}{2}} u,$$

so $\mathbb{X}$ is defined by

$$|u| \geq \left|\varpi^{\frac{-p}{2}}\right|, \text{ or } \left|\frac{1}{u}\right| \leq \left|\varpi^{\frac{p}{2}}\right|.$$

We claim that all the zeroes of u lie outside R. Indeed, $u = 0$ implies $x = -a/c$, and hence $y = (a^a b^b c^c)^{1/p}\zeta$ for some $\zeta \in \mu_p$. Hence

$$|v| = \left|\frac{\zeta - 1}{\varpi}\right| = 1.$$

Thus the zeroes lie in the residue classes of points on the finite portion of the Artin-Schreier curve (20). However, R is the residue class of the point at infinity. This proves the claim. Also, the poles of u coincide with the poles of x, which has a pole of order p at infinity and no others. Thus, $1/u$ is a function on R with no poles, a zero of order p, and no other zeroes; further, since, by Eq. (20), $\tilde{u}$ is a non-zero element of the function field of the special fiber of the smooth model, $1/u$ has spectral norm 1 on R. Thus there exists a parameter W on R such that

$$\frac{1}{u} = W^p(1 + a_1 W + \cdots), \quad |a_i| \leq 1.$$

Hence $\mathbb{X}$ is cut out by the inequality

$$|W| \leq \left|\varpi^{\frac{1}{2}}\right|.$$

The statement for $\mathbb{X}'$ (which is not needed in this paper) follows from a similar argument, using the fact that $\tilde{v}$ has degree two and a double zero in the residue class of $(0,0)$, that $t = \varpi v$, and that $\mathbb{X}'$ is defined by $|t| \leq |p|$.

7. Power series expansions

In this section we assume $F_{a,b,c}$ is wild. Our aim is to calculate power series expansions on the affinoid $\mathbb{X}$ of the function x and a general differential ω. Recall the notation for the three trivial points on on $F_{a,b,c}$: $A = (0,0)$, $B = (1,0)$, and $C = \infty$. Recall also that $\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}$ has geometric genus 0 and exactly one singular point ξ; it is the unique point such that $\tilde{x}(\xi) = -\tilde{a}/\tilde{c}$.

Lemma 14. *Let*

$$\tilde{S}\text{: normalization of } \tilde{\mathcal{F}}^{reg}_{a,b,c} \simeq \mathbb{P}^1$$

be the isomorphism of algebraic curves which maps the triple $(\tilde{A}, \tilde{B}, \tilde{C})$ *to* $(0, 1, \infty)$. *Then*

$$\tilde{S}(\xi) = -\frac{\tilde{a}}{\tilde{c}}.$$

Proof. Since the divisor of $\tilde{x}$ is $p\tilde{C} - p\tilde{A}$, we have an equality of divisors

$$(\tilde{x}) = p(\tilde{S}).$$

Further, $\tilde{x}(\tilde{B}) = \tilde{S}(\tilde{B}) = 1$, so $\tilde{x} = \tilde{S}^p$. Hence $\tilde{S}(\xi)^p = \tilde{x}(\xi) = -\tilde{a}/\tilde{c}$, and so $\tilde{S}(\xi) = -\tilde{a}/\tilde{c}$ also.

Next we need to find a convenient parameter on the affinoid $\mathbb{X}$, which, we recall, is the subspace of $F_{a,b,c}$ which reduces to the open subset $\tilde{\mathcal{F}}^{reg}_{a,b,c} - \xi$.

Lemma 15. *There exists a rigid analytic isomorphism*

$$T\colon \mathbb{X} \simeq \mathbb{B}[1],$$

defined over $\mathbb{Q}_p$, *such that*

$$\begin{aligned} T(A) &= 0, \\ T(B) &= 1, \\ T(C) &= -\frac{b}{c}. \end{aligned}$$

Proof. Let

$$\tilde{T}\text{ : normalization of } \tilde{\mathcal{F}}^{reg}_{a,b,c} \simeq \mathbb{P}^1_{\mathbb{F}_p}$$

be the isomorphism of algebraic curves which maps the triple $(\tilde{A}, \tilde{B}, \xi)$ to $(0, 1, \infty)$. By Lemma 14, $\tilde{S}(\xi) = -\tilde{a}/\tilde{c}$. Thus

$$\tilde{T} = \frac{-\tilde{b}\tilde{S}}{\tilde{c}\tilde{S} + \tilde{a}} \quad (\text{recall } a + b + c = 0),$$

and so $\tilde{T}(\tilde{C}) = -b/c$.

First, $\tilde{T}$ lifts to a parameter T on $\mathbb{X}$, defined over $\mathbb{Q}_p$; indeed, if T' is a parameter on $\mathbb{X}$ defined over $\mathbb{Q}_p$, then $\tilde{T}|_{\tilde{\mathbb{X}}}$ and $\tilde{T}'|_{\tilde{\mathbb{X}}}$ are both isomorphisms to $\mathbb{A}^1$, so $\tilde{T} = \tilde{u}\tilde{T}' + \tilde{v}$, $\tilde{u}, \tilde{v} \in \mathbb{F}_p$, $\tilde{u} \neq 0$. Choose liftings $u, v \in \mathbb{Z}_p$ of $\tilde{u}$ and $\tilde{v}$; then $T = uT' + v$ is a parameter on $\mathbb{X}$ lifting $\tilde{T}$ and defined over $\mathbb{Q}_p$. Now $T(A) \equiv 0$ modulo p and $T(B) \equiv 1$ modulo p. Hence, replacing T by $(T - T(A)/(T(B) - T(A))$, we may suppose that $T(A) = 0$, $T(B) = 1$. (Note that this does not change $\tilde{T}$.) Finally, since

$$\tilde{T}(\tilde{C}) \equiv -b/c \not\equiv 0, 1 \pmod{p},$$

we may multiply T by the unit power series

$$1 - \left(\frac{\frac{b}{c} + T(C)}{T(C)^2(T(C) - 1)} \right) T(T - 1)$$

to obtain a parameter with the same values as T at A and B, and with the value $-b/c$ at C.

Now we will compute the power series expansion of x in T, modulo p^2. Let

$$\phi(U,V) = \frac{(U+V)^p - U^p - V^p}{p}.$$

Proposition 9. *In terms of the parameter T in Lemma 15, we have*

$$x = u\frac{T^p}{(1+\frac{c}{b}T)^p}(1+pf(T)), \quad u \in \mathbb{Q}_p^*, f(T) \in T\mathbb{Z}_p[[T]], \tag{21}$$

where

$$f(T) \equiv \frac{b}{a}(\phi(1,-T) - \phi(1,\frac{c}{b}T) + \phi(\frac{a}{b},1)T^p) \pmod{p}.$$

Proof. Equation (21) holds for some $f(T) \in T\mathbb{Z}_p[[T]]$, simply because x has a zero of order p at A, a pole of order p at C, and no other poles or zeroes. Since y has order a at A, b at B, and c at C, we similarly have

$$y = vT^a(1-T)^b(1+c/bT)^c(1+pg(T)), \quad v \in \mathbb{Q}_p^*, g(T) \in T\mathbb{Z}_p[[T]]. \tag{22}$$

Substituting Eqs. (21) and (22) into Eq. (2), and clearing powers of T and $(1+(c/b)T)$, we get

$$v^p(1-T)^{pb}(1+pg(T))^p = u^a(-1)^c(1+pf(T))^a((1+\frac{c}{b}T)^p - uT^p(1+pf(T)))^b.$$

In particular, setting $T=0$ we get

$$v^p = (-1)^c u^a,$$

so $u \in \mathbb{Q}_p^{*p}$. Also, looking at the equation mod p, we get

$$(1-T^p)^b \equiv (1+\frac{c}{b}T^p - uT^p)^b \pmod{p},$$

so

$$u \equiv \frac{c}{b} + 1 \equiv \frac{-a}{b} \pmod{p}.$$

Since $u \in \mathbb{Q}_p^{*p}$, we therefore have

$$u \equiv \left(\frac{-a}{b}\right)^p \pmod{p^2}.$$

Thus, modulo p^2, we have

$$\begin{aligned}
(1-T)^{pb} &\equiv (1+paf(T))((1+\frac{c}{b}T)^p - uT^p(1+pf(T)))^b \\
&\equiv (1+paf(T))(1+p\phi(1,\frac{c}{b}T) + ((\frac{c}{b})^p + (\frac{a}{b})^p)T^p + (\frac{a}{b})^p pT^p f(T))^b \\
&\equiv (1+paf(T))(1-T^p+p\phi(1,\frac{c}{b}T) - p\phi(\frac{a}{b},1)T^p + p\frac{a}{b}T^p f(T))^b \\
&\equiv (1+paf(T))((1-T^p)^b \\
&\qquad + b(1-T^p)^{b-1}p[\phi(1,\frac{c}{b}T) - \phi(\frac{a}{b},T)T^p + \frac{a}{b}T^p f(T)]) \\
&\equiv (1-T^p)^{b-1}(1-T^p+pb\phi(1,\frac{c}{b}T) - pb\phi(\frac{a}{b},T)T^p + paT^p f(T) \\
&\qquad + paf(T) - T^p paf(T)) \pmod{p^2}.
\end{aligned}$$

On the other hand,

$$(1-T)^{pb} = (1-T^p+p\phi(1,-T))^b$$
$$\equiv (1-T^p)^b + pb(1-T^p)^{b-1}\phi(1,-T) \pmod{p^2}.$$

Equating both sides and dividing by $(1-T)^{b-1}$, we get

$$1-T^p+bp\phi(1,-T) \equiv 1+paf(T)+pb\phi(1,\frac{c}{b}T) -$$
$$pb\phi(\frac{a}{b},T)T^p + paT^pf(T) - T^ppaf(T) - T^p \pmod{p^2},$$

yielding

$$f(T) \equiv \frac{b}{a}(\phi(1,-T) - \phi(1,\frac{c}{b}T) + \phi(\frac{a}{b},1)T^p).$$

Next we observe some general properties of the expansion of a differential ω in T.

Proposition 10. *Let $\omega \in H^0(\mathcal{F}^{reg}_{a,b,c}, \Omega_{\mathcal{F}^{reg}_{a,b,c}/\mathbb{Z}_p})$, and let λ_ω be the Coleman integral of ω. Let T be the parameter on $\mathbb{X}$ given by Lemma 15. The expansion of $\lambda|_{\mathbb{X}}$ as a power series in T has coefficients in $\mathbb{Z}_p$, and*

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

where $\deg \mu \leq p-2$.

Proof. Write

$$\lambda(T) = \sum_{i=0}^{\infty} a_i T^i.$$

Since both T and λ are rational over $\mathbb{Q}_p$, we have $a_i \in \mathbb{Q}_p$. Thus it suffices to show that

(23) $$|a_i| \leq 1 \text{ for all } i, \quad |a_i| < 1 \text{ for } i > p-2 \text{ and } i \neq p, 2p.$$

In fact it suffices to prove these conditions for any choice of parameter T on $\mathbb{X}$ such that $T(A) = 0$, since if T' is any such parameter, and if the corresponding coefficients in the expansion of λ are denoted by a'_i, then we have

$$T' = \sum_{k=1}^{\infty} b_i T^i, \quad |b_1| = 1, \ |b_i| < 1 \text{ for } i > 1.$$

Hence

$$a_i \equiv b_1^i a'_i \pmod{\mathfrak{m}(a'_0, \ldots, a'_{i-1}))},$$

where $\mathfrak{m}$ is the maximal ideal in the ring of integers of $\mathbb{C}_p$. Thus if the conditions (23) hold for the a'_i, they hold for the a_i.

Let W be the parameter on R in Lemma 13, and suppose further that W has been chosen so that $W(A) = 0$. The restriction of W to $\mathbb{X}$ yields an isomorphism

$$W : \mathbb{X} \to \mathbb{B}[|\varpi^{1/2}|], \quad W(A) = 0.$$

Choose $T' = \varpi^{-1/2}W$, and write

$$\lambda(T') = \sum_{i=0}^{\infty} a_i' T'^i = \sum_{i=0}^{\infty} a_i' \varpi^{-i/2} W^i$$

and

$$\omega = d\lambda = \sum_{i=1}^{\infty} i a_i' T'^{i-1} dT' = \varpi^{-1/2} \sum_{i=1}^{\infty} i a_i' \varpi^{-(i-1)/2} W^{i-1} dW.$$

Since $d\lambda = \omega$ cannot have more than $2g-2 = p-3$ zeroes in R (because it can't have more than that many on the entire curve), the theory of Newton polygons implies that the maximum absolute value of the coefficients of $d\lambda$ expanded in W must occur in degree less than or equal to $p-3$. Also, since ω is defined over $\mathbb{Z}_p$, ia_i' is an integer for all i. Thus, for all $i \geq p-2$, we have

$$\left| i a_i' \varpi^{-(i-1)/2} \right| \leq \max\left\{ \left| k a_k' \varpi^{\frac{-(k-1)}{2}} \right| : 1 \leq k \leq p-2 \right\} \leq \left| \varpi^{\frac{-(p-3)}{2}} \right|.$$

Thus

$$|a_i'| \leq \left| \frac{\varpi^{\frac{i-(p-2)}{2}}}{i} \right|, \quad i \geq p-2.$$

This estimate, combined with the fact that ia_i is an integer, yields the conditions (23) for the a_i', and hence the lemma.

8. Proof of Theorem 4

We want to determine the subspace $V \subset H^0(\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}, \omega_{\tilde{\mathcal{F}}^{\mathrm{reg}}_{a,b,c}/\mathbf{F}_p})$ defined in Sect. 4. The first step is to determine its dimension. Recall that $V = j^*W$, $W \subset H^0(\tilde{A}, \Omega^1_{\tilde{A}/\mathbf{F}_p})$ is the annihilator of $\ker \chi$ under the pairing (11)

$$A(\mathbb{Q}_p)/pA(\mathbb{Q}_p) \times H^0(\tilde{A}, \Omega^1_{\tilde{A}/\mathbf{F}_p}) \to \mathbb{F}_p,$$

and

$$\chi\colon A(\mathbb{Q}_p)/pA(\mathbb{Q}_p) \to A(K_\mathfrak{p})/\pi A(K_\mathfrak{p})$$

is the natural map. We start by analysing the pairing more closely.

Lemma 16. *As an $\mathbb{F}_p$ vector space, $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ has dimension $g+1$ and $H^0(\tilde{A}, \Omega^1_{\tilde{A}/\mathbf{F}_p})$ has dimension g. The kernel of the pairing (11) on the left is two-dimensional, and is the image in $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ of $\mathcal{A}_1(\mathbb{Z}_p) + A(\mathbb{Q}_p)_{\mathrm{tor}}$. The kernel of the pairing on the right is one-dimensional.*

Proof. By Lemma 12, the torsion subgroup of $A(\mathbb{Q}_p)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$; it follows that

$$\dim_{\mathbb{F}_p} A(\mathbb{Q}_p)/pA(\mathbb{Q}_p) = g + 1.$$

The fact that $H^0(\tilde{\mathcal{A}}, \Omega^1_{\tilde{\mathcal{A}}/\mathbb{F}_p}) = T_e(\tilde{\mathcal{A}})$ has dimension g follows from the fact that $\tilde{\mathcal{A}}$ is a smooth variety over $\mathbb{F}_p$ of dimension g.

Now, suppose that $P \in A(\mathbb{Q}_p)$ is such that its image in $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ is in the left kernel of the pairing. Then $\Lambda(P) \in pT_e(\mathcal{A})$. By Lemma 1, $\Lambda(\mathcal{A}_1(\mathbb{Z}_p)) = pT_e(\mathcal{A})$, hence there exists $Q \in \mathcal{A}_1(\mathbb{Z}_p)$ such that $\Lambda(P-Q) = 0$. But then $P-Q$ is in the torsion subgroup of $A(\mathbb{Q}_p)$. This proves that the left kernel is the image of $\mathcal{A}_1(\mathbb{Z}_p)+A(\mathbb{Q}_p)_{\text{tor}}$; it remains to prove that that image is two-dimensional. Since $\mathcal{A}_1(\mathbb{Z}_p) \cap A(\mathbb{Q}_p)_{\text{tor}} = 0$, and $A(\mathbb{Q}_p)_{\text{tor}}$ is one-dimensional, it suffices to show that the image of $\mathcal{A}_1(\mathbb{Z}_p)$ in $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ is one-dimensional. This follows from the fact that the reduction map is a surjective map from the $g+1$-dimensional space $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ onto the g-dimensional space $\tilde{\mathcal{A}}(\mathbb{F}_p) \simeq \mathbb{F}_p^g$. The final assertion of the lemma now follows by elementary linear algebra.

Since $\ker \chi$ has codimension one in $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$, it follows from the last statement in Lemma 16 that W has dimension 1 or 2, depending on whether or not there is an element of the left kernel which complements $\ker \chi$. The following lemma settles this point.

Lemma 17. *The image of* $\mathcal{A}_1(\mathbb{Z}_p) + A(\mathbb{Q}_p)_{tor}$ *in* $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ *is contained in* $\ker \chi$.

Proof. The kernel of χ consists of those elements of $A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ which become divisible by π in $A(K_\mathfrak{p})$.

First, it follows from a theorem of Greenberg [G] that $A(\mathbb{Q}_p)_{\text{tor}}$ becomes divisible by π in $A(K_\mathfrak{p})$. Indeed, it follows from Lemmas 4 and 12 that $A(\mathbb{Q})_{\text{tor}} = A[\pi]$, and Greenberg showed that there is a rational point of order π^3 on $A(K_\mathfrak{p})$.

Second, let $\mathcal{A}'$ be the Néron model of $A \times_{\mathbb{Q}_p} K_\mathfrak{p}$ over $\mathcal{O}_\mathfrak{p}$. By Lemma 1, the logarithm induces isomorphisms

$$\mathcal{A}_1(\mathbb{Z}_p) \simeq pT_e(\mathcal{A}) \tag{24}$$

$$\pi\mathcal{A}'_1(\mathcal{O}_\mathfrak{p}) \simeq \pi^2 T_e(\mathcal{A}'). \tag{25}$$

From the defining property of the Néron model we have a map $\mathcal{A} \times_{\mathbb{Z}_p} \mathcal{O}_\mathfrak{p} \to \mathcal{A}'$, which induces an inclusion

$$T_e(\mathcal{A}) \subset T_e(\mathcal{A}'). \tag{26}$$

It now follows from conditions (24), (25), and (26) that $\mathcal{A}_1(\mathbb{Z}_p) \subset \pi\mathcal{A}'_1(\mathcal{O}_\mathfrak{p}) \subset \pi A(K_\mathfrak{p})$, as required.

Proposition 11. *Let* W *be the annihilator under the pairing (11) of* $\ker \chi$. *Then* W, *and hence* V, *has dimension 2.*

Proof. This follows immediately by elementary linear algebra from Lemmas 16 and 17.

Hence to determine V, we need only find two linearly independent differentials contained in it. The following proposition gives a property of differentials in V which will enable us to pin them down. First, we need some terminology: if D is a divisor on $F_{a,b,c}$, defined over $\mathbb{C}_p$, and if f is a $\mathbb{C}_p$-valued function on a subset of $F_{a,b,c}(\mathbb{C}_p)$ containing the support of D, we define

$$f^*(D) = \prod_{P \in F_{a,b,c}} f(P)^{\mathrm{ord}_P(D)}.$$

and

$$f(D) = \sum_{P \in F_{a,b,c}} \mathrm{ord}_P(D) f(P).$$

Proposition 12. *Let $\tilde{\omega} \in H^0(\tilde{\mathcal{F}}^{reg}_{a,b,c}, \omega_{\tilde{\mathcal{F}}^{reg}_{a,b,c}/\mathbb{F}_p})$, let $\omega \in H^0(\mathcal{F}^{reg}_{a,b,c}, \omega_{\mathcal{F}^{reg}_{a,b,c}/\mathbb{Z}_p})$ be a differential reducing to ω, and let λ_ω be the Coleman integral of ω. Then $\tilde{\omega} \in V$ if and only if*

(27)
$\lambda_\omega(D) \equiv 0 \pmod{p}$ *for all $\mathbb{Q}_p$-rational divisors D of degree zero, prime to (x), such that $x^*(D) \in \mathbb{Q}_p^{*p}$.*

Proof. Recall that $V = \tilde{j}^* W$, where W is the annihilator of $\ker \chi$ under the pairing (11)

$$A(\mathbb{Q}_p)/pA(\mathbb{Q}_p) \times H^0(\tilde{A}, \Omega^1_{\tilde{A}/\mathbb{F}_p}) \to \mathbb{F}_p.$$

It follows from the definition of this pairing that if $\tilde{\eta} \in H^0(\tilde{A}, \Omega^1_{\tilde{A}/\mathbb{F}_p})$, η is a differential reducing to $\tilde{\eta}$, and if λ_η is the Coleman integral of η, then $\tilde{\eta} \in W$ if and only if

$$\lambda_\eta(P) \equiv 0 \pmod{p}$$

for all $P \in \ker \chi$.

Now, $\ker \chi$ consists of all $P \in A(\mathbb{Q}_p)/pA(\mathbb{Q}_p)$ that become divisible by π in $A(K_\mathfrak{p})$. By [M2] this is equivalent to P being representable by a $\mathbb{Q}_p$-rational divisor D of degree zero such that

$$x^*(D) \in K_\mathfrak{p}^{*p}.$$

Since $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$ has order prime to p, and D is rational over $\mathbb{Q}_p$, this is equivalent to

$$x^*(D) \in \mathbb{Q}_p^{*p}.$$

Finally, if D represents P and if $\omega = j^*\eta$, then by functoriality of the Coleman integral we have

$$\lambda_\omega(D) = \lambda_\eta(P), \quad \omega = j^*\eta.$$

Now fix a differential $\tilde{\omega} \in V$, let ω be a differential reducing to $\tilde{\omega}$, and let λ be the Coleman integral of ω, normalized so that $\lambda(A) = 0$. By Proposition 10, λ has a power series expansion $\lambda(T)$ on $\mathbb{X}$ with integer coefficients. Let $\tilde{\lambda}(\tilde{T})$ be the reduction of $\lambda(T)$. The following proposition tells us how to determine $\tilde{\lambda}(\tilde{T})$ from $\tilde{\omega}$.

Proposition 13. *Let* $\omega \in H^0(\tilde{\mathcal{F}}^{reg}_{a,b,c}, \omega_{\tilde{\mathcal{F}}^{reg}_{a,b,c}/\mathbb{F}_p})$, *let* $\omega \in H^0(\mathcal{F}^{reg}_{a,b,c}, \omega_{\mathcal{F}^{reg}_{a,b,c}/\mathbb{Z}_p})$ *be a differential reducing to* ω, *and let* λ_ω *be the Coleman integral of* ω. *Then* $\tilde{\lambda}(\tilde{T})$ *is the unique polynomial in* $\tilde{T}$ *such that*

$$d\tilde{\lambda} = \tilde{\omega}, \tag{28}$$

$$\tilde{\lambda}(\tilde{T}) = \mu(\tilde{T}) + \alpha\tilde{T}^p + \beta\tilde{T}^{2p}, \mu \in \mathbb{F}_p[\tilde{T}], \deg\mu \leq p-1, \alpha, \beta \in \mathbb{F}_p, \tag{29}$$

and

$$\lambda(0) = \lambda(1) = \lambda(-b/c) = 0. \tag{30}$$

Proof. The first property is part of the definition, the second is from Proposition 10, and the third follows from the fact that the divisors $B - A$ and $C - A$ represent torsion points on the Jacobian, and the Coleman integrals vanish on torsion. It is clear that the three properties uniquely determine $\tilde{\lambda}$; indeed, the first two allow for three arbitrary constants, namely α, β, and the constant of integration; these three constants are determined by third property.

Thus to find V it suffices to come up with two linearly independent differentials $\tilde{\omega} \in H^0(\tilde{\mathcal{F}}^{reg}_{a,b,c}, \omega_{\tilde{\mathcal{F}}^{reg}_{a,b,c}/\mathbb{F}_p})$ such that the $\tilde{\lambda}$ determined by conditions (28), (29), and (30) satisfies (27). Recall ([M2], Theorem 3.5) that, since $\tilde{\mathcal{F}}^{reg}_{a,b,c}$ is reduced, the dualizing sheaf $\omega_{\tilde{\mathcal{F}}^{reg}_{a,b,c}/\mathbb{F}_p}$ is canonically isomorphic to the sheaf $\Omega^{reg}_{\tilde{\mathcal{F}}^{reg}_{a,b,c}/\mathbb{F}_p}$ of regular differentials ([S1]). This is the sheaf of Kähler differentials $\tilde{\omega}$ with the property that at every point P on $\tilde{\mathcal{F}}^{reg}_{a,b,c}$, the residue of $\tilde{f}\tilde{\omega}$ is zero whenever $\tilde{f}$ is regular at P.

The first candidate for an element of V is

$$\tilde{\omega}_1 = d\tilde{T}. \tag{31}$$

One readily checks this is a regular differential. It is clearly regular everywhere except possibly at $\tilde{T} = \infty$. But in terms of the parameter $\tilde{U} = 1/\tilde{T}$ at infinity (the cusp on $\tilde{\mathcal{F}}^{reg}_{a,b,c}$) it is $-d\tilde{U}/\tilde{U}^2$. This is regular (in the sense described above) at $\tilde{U} = 0$, because function $\tilde{f}$ that is regular at the cusp has no linear term in U, and hence the residue of $\tilde{f}\tilde{\omega}_1$ is zero. The corresponding $\tilde{\lambda}$, satisfying conditions (28), (29), and (30), is

$$\tilde{\lambda}_1 = \tilde{T} - \tilde{T}^p. \tag{32}$$

This vanishes on all of $\tilde{\mathbb{X}}(\mathbb{F}_p) = A^1_{\mathbb{F}_p}$, so it certainly satisfies condition (27).

The other candidate is

$$\tilde{\omega}_2 = d\tilde{\lambda}_2,$$

where

$$\tilde{\lambda}_2 = \tilde{f}(\tilde{T}) = \frac{b}{a}(\phi(1, -\tilde{T}) - \phi(1, \frac{c}{b}\tilde{T}) + \phi(\frac{a}{b}, 1)\tilde{T}^p). \tag{33}$$

Lemma 18. *With* λ_2 *defined as in Eq. (33), the differential* $d\tilde{\lambda}_2 = \tilde{\omega}_2$ *is regular, and* $\tilde{\lambda}_2$ *satisfies conditions (27), (28), (29), and (30)*

Proof. First, it follows from Proposition 9 that for a $\mathbb{Q}_p$-rational divisor D, $\tilde{\lambda}_2(\tilde{D}) \equiv 0 \mod p$ if $x^*(D) \in \mathbb{Q}_p^{*p}$. Thus $\tilde{\lambda}_2$ satisfies condition (27). Also, $\tilde{\lambda}_2$ satisfies condition (28) by definition; $\tilde{\lambda}_2$ is visibly of the form in Eq. (29); and one can easily check that it satisfies condition (30). It remains to check that $\tilde{\omega}_2$ is in fact a regular differential on $\mathcal{F}^{\mathrm{reg}}_{a,b,c}$. One does this by noting from Eq. (21) that

$$\tilde{\omega}_2 = d\tilde{f} = \tilde{\eta},$$

where

$$\eta = \frac{1}{p}\operatorname{dlog} x - \operatorname{dlog} T + \operatorname{dlog}(1 + \frac{c}{b}T).$$

The right hand side is holomorphic on $\mathbb{X}$, because x has a pole of order p at C and a zero or order p at A, and no other poles or zeroes; T has a simple zero at A and no poles; and $1 + (c/b)T$ has a simple zero at C and no poles. Hence η reduces to a differential which is regular everywhere except perhaps at the singular point ξ, the point where $\tilde{T} = \infty$. At that point poles of $\operatorname{dlog}\tilde{T}$ and $\operatorname{dlog}(1 + \frac{c}{b}\tilde{T})$ cancel, so it suffices to show that the reduction of $\eta = \frac{1}{p}\operatorname{dlog} x$ is regular at ξ. This follows since it is holomorphic on the residue class of ξ. (The fact that a differential holomorphic on a residue class reduces to one regular at the point follows from [M2], 5.1.)

It is easy to see that

$$\tilde{\omega}_1 = d\tilde{T} \quad \text{and} \quad \tilde{\omega}_2 = \tilde{f}'(\tilde{T})d\tilde{T}$$

are linearly independent; hence we have shown that

$$V = \mathbb{F}_p\tilde{\omega}_1 + \mathbb{F}_p\tilde{\omega}_2.$$

We are now ready to conclude the proof of Theorem 4. For $P \in F_{a,b,c}(\mathbb{Q}_p)$, define

$$\tilde{\omega}(\tilde{P}) = (\frac{\tilde{\omega}}{d\tilde{T}})(\tilde{P}).$$

First, one easily checks that

$$f'(0) = 1, f'(1) = \frac{b}{a}, \quad \text{and} \quad f'(\frac{-b}{c}) = \frac{c}{a}.$$

Hence, if $\tilde{\omega} \in V$, then

$$(\tilde{\omega}(\tilde{A}), \tilde{\omega}(\tilde{B}), \tilde{\omega}(\tilde{C})) = \text{linear combination of } (a, b, c) \text{ and } (1, 1, 1).$$

Thus $\tilde{\omega}$ cannot vanish at all three points, since a, b, and c are not all equal modulo p, unless $p = 3$ (recall $a + b + c = 0$). This proves the first statement in Theorem 4.

For the second, express $\tilde{f}$ in terms of the parameter $\tilde{S}$:

$$\tilde{f}(\tilde{S}) = \frac{\phi(1, -\tilde{S})}{(1 + \frac{c}{a}\tilde{S})^p}. \tag{34}$$

Then

$$f'(\tilde{S}) = \frac{-\phi'(1, -\tilde{S})}{(1 + \frac{c}{a}\tilde{S})^p}.$$

Now

$$\phi'(1, -\tilde{S}) = (1 - S)^{p-1} - S^{p-1}.$$

Every element of $\mathbb{F}_p$ except 0 and 1 is a simple root of this; thus $\tilde{\omega}_2$ has a simple zero in each first case residue class. Since $\tilde{\omega}_1 = d\tilde{T}$ does not vanish at all in any first case residue class, this proves the second statement of Theorem 4.

References

[AHB] Adelman, L. M., Heath-Brown, D. R., *The first case of Fermat's last theorem*, Invent. Math. **79** (1985), no. 2, 409-416.

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

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Springer-Verlag, Berlin-Heidelberg, 1990.

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

[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] R.F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), 765-770.

[E] L. Euler, *Vollständige Anleitung zur Algebra*, Royal Acad. of Sciences, St. Petersburg, 1770. Also in *Opera Omnia*, Ser. I, Vol. I, Teubner, Leipzig-Berlin, 1915, pp. 484-489.

[F] 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.

[G] R. Greenberg, *On the Jacobian variety of some algebraic curves*, Compos. Math. **42** (1981), 345-359.

[GR] B.H. Gross, D.E. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Invent. Math **44**, 201-224.

[H] R. Hartshorne, *Residues and duality*. Lecture Notes in Mathematics, Vol. 20. Springer, Berlin-Heidelberg-New York, 1966.

[K] E. Kummer, *Beweis des Fermat'schen Satzes der Unmöglichkeit von $x^\lambda + y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen λ*, Monatsber. Akad. Wiss. Berlin (1847), 132-139. In *Collected Papers, I*, 274-281.

[Ma] H. Matsumura, *Commutative Algebra*, Benjamin, Reading, 1980.

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

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

[M3] W.G. McCallum, *The arithmetic of Fermat curves*, to appear in Math. Annalen.

[Mi1] J. S. Milne, *Étale Cohomology*, Princeton University Press, Princeton, 1980.

[Mi2] J. S. Milne, *Arithmetic Duality Theorems*, Academic Press, Orlando, 1986.

[Mi3] J. S. Milne, *Jacobian Varieties*, in G. Cornell and J. H. Silverman, *Arithmetic Geometry*, Springer-Verlag, New York, 1986.

[Ra] M. Raynaud, *Spécialization du Foncteur Picard*, Publ. I.H.E.S. **38** (1970), 27-76.

[Ri] Paulo Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York, 1979.

[S1] J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann, Paris, 1959.

[S2] J.-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

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

This article was processed by the author using the LaTeX style file *pljour1* from Springer-Verlag.