TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 311, Number 1, January 1989

TORSION POINTS ON ABELIAN ÉTALE COVERINGS OF $\mathbf{P}^1 - \{0, 1, \infty\}$

ROBERT F. COLEMAN

ABSTRACT. Let $X \to \mathbf{P}^1$ be an Abelian covering of degree m over $\mathbf{Q}(\mu_m)$ unbranched outside $0, 1$ and ∞. If the genus of X is greater than 1 embed X in its Jacobian J in such a way that one of the points above $0, 1$ or ∞ is mapped to the origin. We study the set of torsion points of J which lie on X. In particular, we prove that this set is defined over an extension of $\mathbf{Q}$ unramified outside $6m$. We also obtain information about the orders of these torsion points.

INTRODUCTION

Suppose $f: X \to \mathbf{P}^1_{\mathbf{Q}(\mu_m)}$ is a Galois morphism of curves over $\mathbf{Q}(\mu_m)$, unbranched outside $\{0, 1, \infty\}$ with Abelian Galois group of exponent m. Then $C = f^{-1}\{0, 1, \infty\}$ is contained in a torsion packet T (see [C-1, C-2 or C-3]). We call the elements of C, the cusps of X and T, the cuspidal torison packet. The group of divisor classes on X represented by divisors of degree zero supported on T is finite and Abelian. We define the exponent of T to be the exponent of this group. In this paper we will prove:

Theorem A. (i) *If the genus of X is at least 2 then the exponent of T divides a power of $2m$.* (ii) *If in addition X is not hyperelliptic then the exponent divides 2 times a power of m.*

We also prove that conjecture B of [C-3] holds for the pair (X, T). In this case, the conjecture is equivalent to the assertion:

Theorem B. *The extension $\mathbf{Q}(T)/\mathbf{Q}$ is unramified outside $6m$.*

The technique of proof is that developed in [C-1 and C-3]. See also [C-2] where more precise, less general, results are proven.

The factor of 2 in case (ii) of Theorem A is probably an anomaly in general, and we can eliminate it in many cases (see Theorem 9 below). However, as we shall show in §VIII, it is really necessary for Klein's twisted quartic, $X^3Y + Y^3Z + Z^3X = 0$ in $\mathbf{P}^2_{\mathbf{Q}(\mu_7)}$, which is a cyclic septic covering of $\mathbf{P}^1_{\mathbf{Q}(\mu_7)}$, unbranched outside $\{0, 1, \infty\}$, via the function $-X^2Y/Z^3$. In fact we show

Received by the editors August 28, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 16B99, 14H40.

the exponent of T, in this case, is 14 and $\#T = 24$, which contradicts Theorem 5.3 if [C-1]. (It is only valid for $p > 2$.)

A brief description of the contents of this paper follows. In §I, we recall and prove some results on PCM de Rham F-crystals, especially applicable to cyclic Fermat quotients. Denote such a quotient by F and its cuspidal torsion packet by T. In §II, we apply the results of [C-3] to F. Essentially, we prove Theorem B for the elements of T which are "far from the cusps" (Proposition 5). In §III, we use the results of §I to analyze T "near the cusps" and complete the proof of Theorem B for T (Proposition 6). We actually prove more and obtain information about when it is ramified above 2 or 3. This leads us to investigate when F has hyperelliptic or ordinary reduction, which we do in §§IV and VI. In §§V and VI we deduce Theorem A for T (Theorem 9) from Propositions 5 and 6 together with the theory of complex multiplication of Abelian varieties due to Shimura-Taniyama and results of [F, G-R, and K-R]. In §VII, we deduce Theorem A, in general, from Theorem 9 and Proposition 6. In §VIII, we investigate the cuspidal torsion packet on Klein's twisted quartic. We also give a simple proof, inspired by Klein's [K] that this is the unique curve over the complex numbers of genus 3 with 168 automorphisms.

I. PCM de Rham F-crystals

This section is rather technical, and may be skipped until it is needed in §III.

We will employ the language and results of [C-3]. Let p be a fixed rational prime, $\mathbf{Q}_p$ the field of p-adic numbers, $\mathbf{C}_p$ the completion of a fixed algebraic extension of $\mathbf{Q}_p$, and K the closure of the maximal unramified algebraic closure of $\mathbf{Q}_p$ in $\mathbf{C}_p$. Let v denote the valuation on $\mathbf{C}_p$ such that $v(p) = 1$. Let R denote the ring of integers in K and $\mathbf{F}$ the residue field of K, so that $\mathbf{F}$ is an algebraic closure of $\mathbf{F}_p$. We let σ denote the absolute Frobenius automorphism of both K and $\mathbf{F}$. Let C be a fixed smooth complete curve over R. We let $\widetilde{C}$ denote the special fiber of C. By a residue class of C we mean a point in $C(\mathbf{F})$ which we also think of as the analytic disk of points in $C(\mathbf{C}_p)$ which reduce to this point. We let $H^1_{\mathrm{dR}}(C)$ denote the first de Rham cohomology module of C over R and $\Omega(C)$ denote the global sections of $\Omega^1(C/R)$, the sheaf of differentials on C over R. We identify $\Omega(C)$ with its image in $H^1_{\mathrm{dR}}(C)$ under the canonical map. We let F and V denote the canonical σ and σ^{-1} linear endomorphisms of $H^1_{\mathrm{dR}}(C)$ called Frobenius and Vershebung respectively. (For more details on the nature of F and V see [C-3, §1].)

In particular,

$$FV = VF = p. \tag{1}$$

By a de Rham F-crystal on C we mean a pair $H = (H, W)$ where H is a submodule of $H^1_{\mathrm{dR}}(C)$ and $W \subseteq H$ is a direct summand of $\Omega(C)$ such that $FH \subseteq H$. It follows from (1) that $VH \subseteq H$. Now suppose that H is a fixed PCM de Rham F-crystal on C. This means it is furnished with a direct sum decomposition of W into rank one R-modules;

$$W = \bigoplus_{i \in I} B_i$$

where I is an index set of cardinality equal to the rank of W over R, such that if $b \in \bigcup_{i\in I} B_i \overset{\text{def}}{=} B$ and $r, k \in \mathbf{Z}$ such that $c = p^{-k}V^r(b) \in H$ and $\tilde{c} \in \widetilde{W}^* = \widetilde{W} - \{0\}$, then $c \in B$. As explained in [C-3], if H is the pullback of the first cohomology module of a CM Abelian scheme over R via a smooth morphism, then H is a PCM de Rham F-crystal.

We will now introduce some notation for the features of a Newton polygon. Suppose

$$f(T) = \sum_{n=0}^{\infty} a_n T^n \in \mathbf{C}_p[[T]].$$

If $f(T) \neq 0$, the Newton polygon of $f(T)$, denoted $N(f)$, is the lower convex hull in the Cartesian plane of the points: $\{(n, v(a_n)): n \geq 0\}$. By a slope of $N(f)$ we mean the slope of one of its sides or $-\infty$ if $a_0 = 0$. A minus slope is the additive inverse of a slope $(-(-\infty) = \infty)$.

Now fix a residue class U of C and a point $Q \in U(R)$. Fix $b \in B$ such that $\tilde{b} \neq 0$. Let $0 = n_0 < n_1 < \cdots < n_1 < \cdots$ be the sequence of integers such that $V^{n_i} b \in B$. This sequence is infinite by Lemma 6 of [C-3]. Let

$$b_i = p^{i-n_i} V^{n_i} b.$$

Then by Lemma 1 of [C-3] and the definition of PCM, $b_i \in B$, $\tilde{b}_i \neq 0$. Suppose

$$\operatorname{ord}_U \tilde{b}_i = \operatorname{ord}_Q b_i. \tag{2}$$

Let $T: U \xrightarrow{\sim} B(0, 1)$ be a uniformizing parameter on U over R such that $T(Q) = 0$. For $w \in W$ let L_w denote the unique solution in $K[[T]]$ of

$$L_w(0) = 0, \qquad dL_w(T) = w \quad \text{on } U.$$

(Note: we regard L_w as a power series in T and hence as a function on $B(0, 1)$ and $L_w(T)$ as an analytic function on U.) Set $N(w) = N(L_w)$.

Let $k_i = 1 + \operatorname{ord}_U \tilde{b}_i$ and set $Q_i = (k_i p^{n_i}, -i)$. By the proof of Proposition 12 of [C-3], $N(b)$ is the lower convex hull of the set of points $\{Q_i: (k_i, p) = 1\}$ and by Lemma 11 of [C-3], if p divides k_i then

$$n_{i+1} = n_i + 1, \quad k_i = pk_{i+1}, \tag{3}$$

$$Q_{i+1} = (k_i p^{n_i}, -(i+1)). \tag{4}$$

Lemma 1. *Suppose there exists a positive integer m such that*

(i) $k_i < m$ *for all* $i \geq 0$,

(ii) $k_i p^{n_i} \equiv k_j p^{n_j} \bmod m$ *for all* $i, j \geq 0$.

Then $k_i p^{n_i} \leq k_j p^{n_j}$ *if* $i \leq j$.

Proof. Suppose $i \leq j$, then since $n_j \geq n_i$, (ii) implies

$$k_1 = k_j p^{n_j - n_i} + am$$

for some integer a. Now (i) implies $a \leq 0$. Hence

$$k_i p^{n_i} = k_j p^{n_j} + amp \leq k_j p^{n_j}.$$

This completes the proof.

We will assume

$$k_i p^{n_i} \leq k_j p^{n_j} \quad \text{when } i \leq j$$

for the rest of this section.

Lemma 1.5. *If we assume in addition to the hypotheses of Lemma 1 that $p > m$ then the set of Q_i's is the set of vertices of $N(w)$.*

Proof. This comes down to proving $\mathrm{slope}(\overrightarrow{Q_iQ_j}) < \mathrm{slope}(\overrightarrow{Q_jQ_n})$ if $0 \leq i < j < n$ are integers. If we set $n - j = r$ and $j - i = s$ this becomes

$$sp^s(k_n p^r - k_j) > r(k_j p^s - k_i).$$

Now because $0 < k_j < m$ we have

$$r(k_j p^s - k_i) < rmp^s,$$

also

$$sp^s(k_n p^r - k_j) = sp^s[k_n p^r/m]m \geq [p^r/m]p^s m.$$

The lemma now follows from the inequality $[p^r/m] \geq r$ for $r \geq 1$ as $p > m$. □

Suppose $0 < i_1 < \cdots < i_j < \cdots$ is the sequence of positive integers such that Q_{i_j} is a vertex of $N(b)$ for $j > 0$. Set $i_0 = 0$. If Q_0 is not a vertex, then i_1 is the smallest natural number such that $(k_{i_1}, p) = 1$. This number exists by (3).

Lemma 2. *Suppose Q_{i_t} is a vertex of $N(b)$, $i_t \leq l < i_{t+1}$ for some integers l and $t \geq 0$. Then the set of vertices of $N(b_l)$ is*

$$A \cup \{(k_{i_j} p^{n_{i_j} - n_l}, l - i_j) : j > t\}$$

where

$$A \subseteq \{(k_i p^{n_i - n_l}, l - i) : i_{t+1} \geq i \geq l, (k_i, p) = 1\}$$

and $A = \{(k_{i_t}, 0)\}$ if $l = i_t$.

Proof. Set $Q_{l,i} = (k_i p^{n_i - n_l}, l - i)$. Then $N(b_l)$ is the lower convex hull of the set of these points and

$$\mathrm{slope}(\overrightarrow{Q_{l,i}Q_{l,j}}) = p^{n_l}\mathrm{slope}(\overrightarrow{Q_iQ_j}). \tag{5}$$

The lemma follows from this and the fact that if $l \leq i < j \leq i_{t+1}$ and both $Q_{l,i}$ and $Q_{l,j}$ are vertices of $N(b_l)$ then

$$\mathrm{slope}(\overrightarrow{Q_iQ_j}) \leq \mathrm{slope}(\overrightarrow{Q_{i_t}Q_{i_{t+1}}}) \tag{6}$$

with equality only if $i = i_t$ and $j = i_{t+1}$ as the points Q_i and Q_j lie above the segment from Q_{i_t} to $Q_{i_{t+1}}$. $\square$

Let r be the smallest positive integer such that $V^r b \in bR$. This exists since V is injective. Let d be the integer such that $n_d = r$. Let e be the largest integer such that $i_e \leq d$.

Lemma 3. *We have*

$$n_{i+d} = n_i + r \tag{7}$$

and

$$i_{j+e} = i_j + d. \tag{8}$$

Proof. Suppose $s, t \in \mathbf{N}$, $0 \leq s < r$. Then $V^{tr+s}(b) \in V^s(b)R$ so $V^{tr+s}(b) \in B$ iff $V^s(b) \in B$ iff $s = n_i$ for some $0 \leq i < d$. Hence if $j, f > 0$ are the integers such that $tr = n_j$, $(t+1)r = n_{j+f}$ then we must have

$$n_{j+i} = tr + n_i$$

for $0 \leq i < f$ and also that $f = d$. Statement (7) follows immediately by induction from this.

Now since $bR = b_d R$ we have $N(b) = N(b_d)$. Note that $i_e \leq d < i_{e+1}$. Lemma 2 implies

$$\begin{aligned} n_{i_j} &= n_{i_{e+j}} - n_d, \qquad j > 0, \\ &= n_{i_{e+j}} - r. \end{aligned}$$

So by (7), $n_{i_j+d} = n_{i_{j+e}}$ and hence $i_j + d = i_{j+e}$, since the n_i are strictly increasing with i. This proves (8).

Lemma 4. *Suppose s is a common finite minus slope of the $N(b_i)$, $i \geq 0$. Then $d = e$, $i_j = j$, $k_i \equiv k_j \not\equiv 0 \bmod p$ for all $i, j \geq 0$, $s^{-1} \in \mathbf{Z}$ and*

$$-s^{-1} \equiv p^r k_0 \mod p^{r+1} \tag{9}$$

for some $r \in \mathbf{N}$.

Proof. First, in view of Lemma 2, after replacing b with b_{i_1} if necessary we may suppose Q_0 is a vertex of $N(b)$. The minus slopes of $N(b)$ are s_j, $j \geq 1$, where

$$s_j = -\text{slope}(\overrightarrow{Q_{i_j} Q_{i_{j+1}}}).$$

By Lemma 3,

$$s_{j+e} = p^{-r} s_j. \tag{10}$$

Now suppose $i_t \leq l < i_{t+1}$. Then by Lemma 2 the minus slopes of $N(b_l)$ are either of the form

$$-\text{slope}(\overrightarrow{Q_{l, i_j} Q_{l, i_{j+1}}}) = p^{n_l} s_j$$

for $j > t$ or $j = t$ and $l = 4$ (using (5)), or of the form

$$-\mathrm{slope}(\overrightarrow{Q_{l,i}Q_{l,j}}) \tag{11}$$

if $l > i_t$ and $l \leq i < j \leq i_{t+1}$ are such that $Q_{l,i}$ and $Q_{l,j}$ are vertices of $N(b_l)$. If $i_t < l < i_{t+1}$ then inequality (6) implies no minus slope of the form (11) is a common slope of both $N(b_l)$ and $N(b_{i_t})$ since the minus slopes of the form (11) are all strictly greater than those of $N(b_{i_t})$.

We conclude from this that s is of the form $p^{n_l}s_{j_l}$ for each l and some j_l such that $i_{j_l} \geq l$. Hence

$$s_{j_l} = p^{-n_l}s_{j_0}. \tag{12}$$

Now,

$$s_{j_0} > p^{-n_1}s_{j_0} > \cdots > p^{-n_{d-1}}s_{j_0} > p^{-r}s_{j_0}. \tag{13}$$

But, (8) implies $N(b)$ has exactly e minus slopes m such that $s_{j_0} \geq m > p^{-r}s_{j_0}$. Hence by (12) and (13), $d = e$ and $i_j = j$. It follows that

$$s_j = \frac{1}{k_{j+1}p^{n_{j+1}} - k_j p^{n_j}}.$$

and $s_j = p^{-n_j}s_0$. This and (12) imply (9). This completes the proof.

Corollary 4.1. *If s is a common finite minus slope of $N(w)$, $w \in W$, then $s^{-1} \in \mathbf{Z}$ and $s^{-1} - 1 \equiv \mathrm{ord}_Q b \bmod p$ for all $b \in B$.*

II. Cyclic Fermat quotients

Let m be a fixed positive integer. Let F_m denote the complete projective scheme over $\mathbf{Z}$ by the homogeneous equation

$$X^m + Y^m + Z^m = 0.$$

The finite flat group scheme over $\mathbf{Z}$,

$$G_m = \frac{\mu_m \times \mu_m \times \mu_m}{\Delta}$$

acts on F coordinatewise, where Δ is the diagonal copy of μ_m in μ_m^3. Let a, b and c be integers such that $a+b+c = 0$. Let $H_{a,b,c} = H^m_{a,b,c}$ be the subgroup scheme of G_m whose $\overline{\mathbf{Q}}$ points are represented by triples $(\xi_1, \xi_2, \xi_3) \in \mu_m(\overline{\mathbf{Q}})^3$ such that $\xi_1^a\xi_2^b\xi_3^c = 1$. Then $H_{a,b,c}$ is finite and flat over $\mathbf{Z}$ and we may define the quotient scheme

$$F_{a,b,c} = F^m_{a,b,c} = F_m/H_{a,b,c}$$

over $\mathbf{Z}$. The group scheme

$$G_{a,b,c} = G^m_{a,b,c} = G_m/H_{a,b,c}$$

acts on $F_{a,b,c}$. When $(m, a, b, c) = 1$, we call these cyclic Fermat quotients. They are cyclic in two ways. The Fermat curve F_m is a potentially cyclic covering of degree m of $F_{a,b,c}$ and $F_{a,b,c}$ is a potentially cyclic covering of degree m of $\mathbf{P}^1$. For the rest of this section we suppose a, b, c are fixed so that $(m, a, b, c) = 1$. This implies that $H_{a,b,c} \cong \mu_m$, and F has the affine equation

$$w^m = (-1)^c u^a (1-u)^b .$$

The map $f_{a,b,c}$ from F_m to $F_{a,b,c}$ is now given by

$$w = X^a Y^b Z^c \quad \text{and} \quad u = -(X/Z)^m .$$

Clearly

$$H_{a,b,c} = H_{a',b',c'} \tag{1}$$

if $(a, b, c) = t(a', b', c') \bmod m$ for some $t \in \mathbf{Z}$, $(t, m) = 1$. Also, the evident action of S_3 on F_m yields

$$F_{a,b,c} \cong F_{a',b',c'} \tag{2}$$

if $\{a, b, c\} = \{a', b', c'\}$. We write

$$(a, b, c) \underset{m}{\sim} (a', b', c')$$

if $\{a, b, c\} \equiv \{ta', tb', tc'\} \bmod m$, for some $t \in \mathbf{Z}$, $(t, m) = 1$. When there is no risk of confusion we write $\sim$ in place of $\underset{m}{\sim}$. From (1) and (2) we see that $F_{a,b,c} \cong F_{a',b',c'}$ if $(a, b, c) \sim (a', b', c')$.

The genus of F is

$$g_{a,b,c} = g^m_{a,b,c} = \tfrac{1}{2}(m - ((m, a) + (m, b) + (m, c)) + 2)$$

from which it follows that $F_{a,b,c}$ has genus zero iff m divides a, b or c and has genus one iff m does not divide a, b or c and $m \leq 4$ or $m = 6$ and 6 divides abc (see [C-M, Lemma 3.2]).

Now let $x = X/Z$, $y = Y/Z$ be functions on F_m. Let

$$\omega_{r,s} = x^r y^s \frac{y}{x} d\frac{x}{y} = x^r y^s \frac{dy}{x^m y}$$

be differentials on F_m. Then $H^0(F_m, \Omega^1_{F_m/\mathbf{Z}})$ is spanned by $\{\omega_{r,s} \colon r > 0, s > 0, r + s < m\}$. Clearly, the $\omega_{r,s}$ are eigendifferentials for the action of G_m with distinct eigencharacters. In particular, it follows that the Jacobian of $F_{a,b,c}$ has CM over $\mathbf{Q}(\mu_m)$ by the image of the group ring $\mathbf{Z}[G_m(\overline{\mathbf{Q}})]$ in its endomorphism ring.

Let $C_m \subseteq F_m(\overline{\mathbf{Q}})$ denote the locus of XYZ on F_m and

$$C_{a,b,c} = u^{-1}\{0, 1, \infty\} \subseteq F_{a,b,c}(\overline{\mathbf{Q}}).$$

Then $f_{a,b,c} C_m = C_{a,b,c}$. We call C_m and $C_{a,b,c}$ the cusps of F_m and $F_{a,b,c}$, respectively. It is well known [Ra, Ro] that C_m and $C_{a,b,c}$ are contained in torsion packets in $F_m(\overline{\mathbf{Q}})$ and $F_{a,b,c}(\overline{\mathbf{Q}})$ which we shall denote by T_m and $T_{a,b,c}$, respectively. Clearly, $T_{a,b,c}$ is stable under $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

If $\omega_{r,s}$ is fixed by $H_{a,b,c}$ then $\omega_{r,s}$ is the pullback of a unique differential $\nu_{r,s}$ on $F_{a,b,c}$. Let

$$L_{a,b} = \{(r,s): 0 \le r < m, 0 \le s < m, br \equiv as \bmod m\},$$
$$L'_{a,b} = \{(r,s) \in L_{a,b}: r, s \text{ and } r+s \text{ are not } 0 \bmod m\},$$
$$L''_{a,b} = \{(r,s) \in L'_{a,b}: r+s < m\}.$$

Then $\{\nu_{r,s}: (r,s) \in L''_{a,b}\}$ is an eigenbasis with distinct eigencharacters for

$$\Omega_{a,b,c} \stackrel{\text{def}}{=} H^0(F_{a,b,c}, \Omega^1(F_{a,b,c}/\mathbf{Z}))$$

under the action of G_m.

For $i \in \mathbf{P}^1_{\mathbf{Q}}(\overline{\mathbf{Q}})$ let r_i be an integer such that $r_0 + r_1 + r_\infty = m$, $(r_0, r_1) \in L_{a,b}$ and $r_i = 1$ if $i \notin \{0, 1, \infty\}$. Then for $P \in F_{a,b,c}(\overline{\mathbf{Q}})$

$$\mathrm{ord}_P \nu_{r_0,r_1} = (r_{u(P)}/(r_{u(P)}, m)) - 1. \tag{3}$$

Moreover, if we regard $u = -x^m$ as a function on F_m then

$$\mathrm{ord}_P \omega_{r_0,r_1} = r_{u(P)} - 1, \tag{4}$$

for $P \in F_m(\overline{\mathbf{Q}})$. Let

$$Z_{a,b,c} = \{P \in F_{a,b,c}(\mathbf{Q}): \nu_{r,s}(P) = 0 \text{ for some } (r,s) \in L''_{a,b}\}.$$

Then it follows that $Z_{a,b,c} \subseteq C_{a,b,c}$.

Assume that $g_{a,b,c} \ge 2$ for the rest of this section. Let p be a fixed rational prime not dividing m. It follows that F_m and $F_{a,b,c}$ have good reduction at p. Let $\mathfrak{p}$ be a fixed prime of $\overline{\mathbf{Q}}$ lying over p. Embed $\overline{\mathbf{Q}}$ in $\mathbf{C}_p$ via $\mathfrak{p}$ and extend scalars to R. As in the proof of Corollary 21.1 of [C-3], it follows that the de Rham F-crystal on $F_{a,b,c}$, $(H^1_{\mathrm{dR}}(F_{a,b,c} \times R/R), \Omega_{a,b,c} \otimes R)$ is PCM with respect to the decomposition

$$\Omega_{a,b,c} \otimes R = \bigoplus_{(r,s) \in L_{a,b}} \nu_{r,s} R.$$

A "$\sim$" superscript will denote reduction mod $\mathfrak{p}$ (not to be confused with our other use of "$\sim$").

Suppose $Q \in T_{a,b,c}$. It follows from Theorems 20 and 21 of [C-3] that

Proposition 5. *The extension $\mathbf{Q}(Q)/\mathbf{Q}$ is unramified above p if one of the following holds*:

(i) *$F_{a,b,c}$ is ordinary at p and $p > 3$ or $p = 2$ and $\widetilde{F}_{a,b,c}$ is not hyperelliptic.*

(ii) *$F_{a,b,c}$ is superspecial at p and $p > 2$ or $\widetilde{F}_{a,b,c}$ is not hyperelliptic.*

(iii) *$F_{a,b,c}$ is extraordinary at p and $\widetilde{Q} \notin \widetilde{Z}_{a,b,c}$.*

III. Analysis at a cusp

We maintain the notations of the previous section. In particular, $(m, a, b, c) = 1$, $g_{a,b,c} \geq 2$, p is a rational prime not dividing m, and $\mathfrak{p}$ is a prime of $\overline{\mathbf{Q}}$ above p. We embed $\overline{\mathbf{Q}}$ into $\mathbf{C}_p$ via $\mathfrak{p}$ and extend scalars from $\mathbf{Z}$ to R without altering our notation unless there is a danger of confusion. We call the sets $\widetilde{C}_m$ and $\widetilde{C}_{a,b,c}$ the cuspidal residue classes of F_m and $F_{a,b,c}$ respectively. We shall prove in this section and the next,

Proposition 6. *If $p > 2$ or $F_{a,b,c}$ is not hyperelliptic, then $T_{a,b,c} \cap \widetilde{Z}_{a,b,c} = Z_{a,b,c}$.*

We wish to apply the results of §1. First, for $\omega \in \Omega_{a,b,c}$ and $P \in C_{a,b,c}$, set

$$\lambda_\omega(Q) = \int_P^Q \omega$$

for $Q \in F_{a,b,c}(\mathbf{C}_p)$. This is independent of the choice of P. Set $T = f_{a,b,c}^{-1}(T_{a,b,c})$. By Theorem 3.1 of [C-1],

$$T = \{Q \in F_{a,b,c}(\mathbf{C}_p) \colon \lambda_\omega(Q) = 0, \omega \in f_{a,b,c}^{*}\Omega_{a,b,c}\}.$$

Now $W := f_{a,b,c}^{*} H_{\mathrm{dR}}^1(F_{a,b,c}/R)$ is a PCM de Rham F-crystal with respect to the decomposition $W = \bigoplus \omega_{r,s} R$ where (r, s) runs over $L''_{a,b}$.

If $Q \in C_m$ then $\mathrm{ord}_Q \omega_{r,s} = \mathrm{ord}_{\widetilde{Q}} \widetilde{\omega}_{r,s}$. Moreover, if $V^n \omega_{r,s} \in \omega_{r',s'} R$ then $p^n (r', s') \equiv (r, s) \bmod m$. Hence it follows that this F-crystal satisfies the hypotheses of Lemmas 1–4. Hence by Lemma 4, if $Q \in C_m$ and $T \cap \widetilde{Q} \neq Q$, then

$$\mathrm{ord}_Q \omega_{r,s} \equiv \mathrm{ord}_Q \omega_{r',s'} \mod p$$

for all (r, s) and $(r', s') \in L''_{a,b}$. By §II(4), if $u(Q) = 0$, this is equivalent to

$$(-1) \qquad\qquad r \equiv r' \mod p$$

for all (r, s) and $(r', s') \in L''_{a,b}$. To understand what this means, we need the following lemma.

Let

$$S'_{a,b} = \{r \colon \text{there is an } s \text{ such that } (r, s) \in L'_{a,b}\},$$
$$S''_{a,b} = \{r \colon \text{there is an } s \text{ such that } (r, s) \in L''_{a,b}\}.$$

For $(r, s) \in L_{a,b}$, let $(r, s)^* = (m - r, m - s)$. Then

$$L''_{a,b} \coprod (L''_{a,b})^* = L'_{a,b}.$$

Lemma 7. *Suppose l is a positive integer which does not divide m and*

$$(0) \qquad\qquad \#(S''_{a,b} \bmod l) = 1;$$

then either $2(m,a) = m$ *and* $S''_{a,b} = \{m/2\}$ *or* $l = 2$ *and* $L_{a,b} = L_{-2,1}$.

Proof. Set $a' = (m,a)$, $b' = (m,b)$, $c' = (m,c)$. First we observe that

$$S'_{a,b} \subseteq \{ia' : 0 < i < m/a'\} \tag{1}$$

and $m \geq 5$, since otherwise $g_{a,b,c} < 2$. We claim $a' \in S''_{a,b}$. There exists an $0 < s \leq m/a$ such that $ba' \equiv as \bmod m$ since $(a/a', m/a') = 1$. Now $(a', s) \in L_{a,b}$, $a' \neq 0$, and $a' + s \leq a' + m/a' < m$ unless $a' = 1$ since $m > 4$. If $a' = 1$ then $a' + s < m$ unless $s = m - 1$ which would imply $a + b \equiv 0 \bmod m$, a contradiction. Hence $(a', s) \in L''_{a,b}$ so $a' \in S''_{a,b}$, which establishes our claim.

We also claim that if $a' > 1$, and $m/a' > 2$ then $2a' \in S''_{a,b}$. There exists an $0 < s \leq m/a'$ such that $2ba' \equiv as \bmod m$. Hence $(2a', s) \in L_{a,b}$, $2a \not\equiv 0 \bmod m$, and $s \neq 0$. Also,

$$2a' + s \leq 2a' + m/a' < m$$

unless $a' = 3$, $m = 9$ or $a' = 2$ and $m = 6$ or 8. If $a' = 3$, $m = 9$ and $2a' + s \geq m$ then $s = 3$ so that 3 divides b, a contradiction. We obtain a similar contradiction if $a' = 2$ and $m = 8$. If $a' = 2$ and $m = 6k$, then $2a' + s \geq m$ implies $s = 2$ or 3. In the former case 3 divides c and in the latter case 3 divides b. Hence in either case $g_{a,b,c} < 2$, a contradiction. This establishes the claim.

At this point, we conclude that if $a' > 1$ and $m/a' > 2$ then $\{a', 2a'\} \subseteq S''_{a,b}$ so that we must have $a' \equiv 2a' \bmod l$. As l does not divide m, this is impossible. Hence we must have either $a' > 1$, $m/a' = 2$ or $a' = 1$.

Suppose $a' > 1$, $m/a' = 2$. Then it follows from (1) that $S'_{a,b} = S''_{a,b} = \{a'\}$ which yields the lemma in this case.

Finally, suppose $a' = 1$. Then as we checked above, there is an $0 < s \leq m-2$ such that $(1, s) \in L''_{a,b}$. Let $0 \leq s' < m$ such that $s' \equiv 2s \bmod m$. Then $(2, s') \in L''_{a,b}$ unless $s' = 0$ or $m - 2 \leq s' < m$ which implies $m - 2 \leq 2s \leq m$.

If m is odd this implies $s = (m-1)/2$ so

$$L_{a,b} = L_{1,(m-1)/2} = L_{-2,1}$$

and $(3, (m-3)/2) \in L''_{a,b}$ since $m \geq 5$. Hence in this case (0) implies $1 \equiv 3 \bmod l$ so $l = 2$.

If m is even then either $s = m/2$ or $s = (m-2)/2$.

In the first case $(3, m/2) \in L''_{a,b}$ unless $m = 6$ and 6 divides abc so that $g_{a,b,c} < 2$, a contradiction. Hence in this case $1 \equiv 3 \bmod l$ so that $l = 2$ but $(l, m) = 1$, a contradiction.

In the second case, $s = (m-2)/2$, $(3, (m-6)/2) \in L''_{a,b}$ as $g_{a,b,c} \geq 2$. As before $1 \equiv 3 \bmod l$, but this contradicts $l \nmid m$. This completes the proof of the lemma.

Now we are ready to finish the proof of Proposition 6. First, if $2(m,a) = m$, then it follows from §II(3) that the elements Q of $C_{a,b,c}$ with $u(Q) = 0$

are not in $Z_{a,b,c}$. Next suppose that $Q \in Z_{a,b,c}$ such that $u(Q) = 0$ and $T_{a,b,c} \cap \widetilde{Q} \neq Q$. Then, after pulling this statement back to F_m, it follows from (-1) and Lemma 7 that $p = 2$ and $\{a, b, c\} \sim \{-2, 1, 1\}$. The proposition now follows from this, symmetry, and the result to be proven in the next section that $F_{1,1,-2}$ is hyperelliptic.

Remark. The results of the last two sections relied on an analysis of the Newton polygons of the integrals of the differentials $\omega_{r,s}$. Let us summarize here what we now know about these polygons.

Suppose $\omega_{r,s}$ is a holomorphic differential on F_m as above. Let Q be a point on F_m defined over the maximal unramified extension K of $\mathbf{Q}_p$. If $\widetilde{Q} \in \widetilde{C}_m$ we suppose $Q \in C_m$. Let T be a uniformizing parameter on $\widetilde{Q}$ defined over K which vanishes at Q. Let $L(T)$ be a power series in T over K with constant term zero such that $dL(T) = \omega_{r,s}$ on $\widetilde{Q}$. Let (r_n, s_n) be the sequence of pairs of integers such that $0 < r_n, s_n < m$ and

$$p^n(r_n, s_n) \equiv (r, s) \mod m.$$

Then we have

Proposition 7.2. (i) *Suppose $Q \notin C_m$. Then the vertices of the Newton polygon of $L(T)$ are $\{(p^n : -n) : r_n + s_n < m\}$.*

(ii) *Suppose $u(Q) = 0$. Then the Newton polygon of $L(T)$ is the lower convex hull of $\{(r_n p^n, -n) : r_n + s_n < m$ and $(r_n, p) = 1\}$. Moreover, this is the set of vertices of the Newton polygon of L if $p > m$.*

This result follows from the discussion at the beginning of §1, Lemma 1.5 and the results of [C-3].

An example in which the set in (ii) differs from the set of vertices of the Newton polygon of $L(T)$ is $m = 5$, $p = 2$ and $(r, s) = (1, 2)$. From this proposition one can see why the cuspidal residue classes are the rise points, in the sense of [C-3], of F_m, when F_m has extraordinary reduction.

IV. Hyperelliptic cyclic Fermat quotients

Maintain the notation of the preceding two sections.

Proposition 8. *The curve $F_{a,b,c} \times \mathbf{F}_p$ is hyperelliptic iff*

(i) $(a, b, c) \sim (1, 1, -2)$ *or*

(ii) $(a, b, c) \sim (1, n, -(1+n))$ *and* $m = 2n$.

Proof. We first check that the curves listed are hyperelliptic.

Case (i). $F_{1,1,-2}$ has the equation $w^m = u(1-u)$ and $u \mapsto 1-u$, $w \mapsto w$ is the hyperelliptic involution.

Case (ii). Here $m = 2n$, and $F_{1,n,-(1+n)}$ has the equation

$$w^m = u(1-u)^n(-1)^{n+1}.$$

The quotient curve by the involution $(u, w) \mapsto (u, -w)$ has the equation

$$v^n = u(1-u)^n(-1)^{n+1}$$

which, as we observed earlier, has genus zero. Hence $F_{1,n,-(n+1)}$ is hyperelliptic.

Now suppose $F = F_{a,b,c} \times \mathbf{F}_p$ is hyperelliptic. Let τ denote its hyperelliptic involution. Then τ commutes with the action of $G_{a,b,c}$ on F.

Case (i): $\tau \notin G_{a,b,c}(\overline{\mathbf{F}}_p)$. This means τ acts nontrivially on $F/G_{a,b,c}$ which is the u-line. Moreover it must permute the branch locus, $\{0, 1, \infty\}$. By symmetry we may suppose it fixes ∞. It follows that $\tau(u) = 1 - u$ and so $a = b$ and $(a, b, c) \sim (1, 1, -2)$.

Case (ii): $\tau \in G_{a,b,c}(\overline{\mathbf{F}}_p)$. Since $G_{a,b,c} \cong \mu_m$ it follows that $m = 2n$ and $\tau(u, w) = (u, -w)$. Now $F_{a,b,c}/\langle\tau\rangle$ has the equation

$$v^n = u^a(1-u)^b(-1)^c.$$

This must have genus zero so n must divide a, b, or c. By symmetry we may suppose n divides b. Since m does not divide b, $b \equiv n \bmod m$. Since $(m, a, b, c) = 1$, we must have $(m, a) = 1$ or $(m, b) = 1$. By symmetry, we may suppose $(m, a) = 1$. Then $(a, b, c) \sim (1, n, -(1+n))$ as required. This completes the proof.

Corollary 8.1. *$F_{a,b,c} \times \mathbf{F}_p$ is hyperelliptic iff $F_{a,b,c} \times \mathbf{Q}$ is hyperelliptic.*

Corollary 8.2. *For a given positive integer m, there are at most 9 hyperelliptic cyclic Fermat quotients. This maximum is achieved iff $m = 2n$ and $n > 2$.*

V. Torsion points on cyclic Fermat quotients

It is the aim of this section and the next to prove

Theorem 9. (i) *The exponent of $T^m_{a,b,c}$ divides a power of $2m$.*

(ii) *If $F^m_{a,b,c}$ is not hyperelliptic, the exponent divides 2 times a power of m.*

(iii) *If, in addition to the hypothesis of* (ii), $(m, 21) = 1$ *or* $(m, 3) = 1$ *and* $(a, b, c) \not\sim (1, 2, -3)$ *then the exponent divides a power of m.*

Our first task is to prove the following proposition.

We now fix m and a, b, c. Let $f_m(x)$ denote the mth cyclotomic polynomial. Let $J_{a,b,c} = J^m_{a,b,c}$ denote the Jacobian of $F_{a,b,c}$ and $J^{\text{new}}_{a,b,c} = (J^m_{a,b,c})^{\text{new}}$ the quotient of $J_{a,b,c}$ by the subabelian variety $f_m(g)J_{a,b,c}$ where g is any generator of $G_{a,b,c}$. This abelian variety is still defined over $\mathbf{Q}$. Then over the field of mth roots of unity, $L = L_m$, $J^{\text{new}}_{a,b,c}$ has *CM* by the ring $\mathbf{Z}[G^m_{a,b,c}(\overline{\mathbf{Q}})]/(f_m(g))$ which is isomorphic to the ring of integers $\mathcal{O} = \mathcal{O}_m$ in

L. Identify the two rings via an isomorphism such that the identity representation of $\mathcal{O}$ is contained in the representation of $\mathcal{O}$ on $H^0(J_{a,b,c}, \Omega^1_{J_{a,b,c}/\mathcal{O}})$. For $(t, m) = 1$ set

$$r(t) = \langle at/m \rangle + \langle bt/m \rangle + \langle ct/m \rangle.$$

Let $\sigma_t \in \mathrm{Gal}(L/\mathbf{Q})$ such that $\zeta^{\sigma_t} = \zeta^t$, $\zeta \in \mu_m$. Then the CM type of $J^{\mathrm{new}}_{a,b,c}$ with respect to $\mathcal{O}$ is

$$\Phi_{a,b,c} = \Phi^m_{a,b,c} = \sum_{t=1}^{m}{}'(r(t) - 1)\sigma_{\varepsilon t}^{-1}$$

where $\varepsilon = (-1)^{r(1)}$ and the $'$ indicates that the summation is taken over indices prime to m. Note that $r(t) - 1 \in \{0, 1\}$.

Proposition 10. *Let p be a rational prime $(p, m) = 1$ and let $Q \in J^{\mathrm{new}}_{a,b,c}(\overline{\mathbf{Q}})$.*

(i) *If the order of Q equals p then $\mathbf{Q}(Q)/\mathbf{Q}$ is ramified above p unless $p = 2$ and $J^{\mathrm{new}}_{a,b,c}$ is ordinary at 2.*

(ii) *If the order of Q equals p^2 then $\mathbf{Q}(Q)/\mathbf{Q}$ is wildly ramified above p.*

Proof. Let $\mathfrak{p}$ be a prime above p in L. It suffices to prove:

(i$'$) If order$(Q) = \mathfrak{p}$ then $L(Q)/L$ is tamely ramified above $\mathfrak{p}$ and is actually ramified above $\mathfrak{p}$ unless $p = 2$ and $J^{\mathrm{new}}_{a,b,c}$ is ordinary at 2.

(ii$'$) If order$(Q) = \mathfrak{p}^2$ then $L(Q)/L$ is wildly ramified above $\mathfrak{p}$.

Let T_p denote the p-Tate module of $J^{\mathrm{new}}_{a,b,c}(\overline{\mathbf{Q}})$. Let $G_{\mathfrak{p}}$ denote the inertia subgroup of $\mathrm{Gal}(\overline{L}/L)^{ab}$ above $\mathfrak{p}$. Then by class field theory we have an isomorphism $A: \mathcal{O}_{\mathfrak{p}}^* \xrightarrow{\sim} G_{\mathfrak{p}}$, where $\mathcal{O}_{\mathfrak{p}}$ is the completion of $\mathcal{O}$ at $\mathfrak{p}$. Hence, we get a map

$$\mathcal{O}_{\mathfrak{p}}^* \to \mathrm{Aut}_{\mathcal{O}_{\mathfrak{p}}}(T_p) \cong \mathcal{O}_p^*$$

where $\mathcal{O}_p = \mathbf{Z}_p \otimes \mathcal{O}$, the completion of $\mathcal{O}$ at p. This map is completely described by $\Phi_{a,b,c}$. Explicitly, this map takes $x \mapsto x^{\Phi_{a,b,c}} \in \mathcal{O}_p^*$ for $x \in \mathcal{O}_{\mathfrak{p}}^*$. If Q is as in (i$'$) or (ii$''$), we deduce $Q^{A(x)} = x^{\Phi_{a,b,c}}Q = x^{\theta}Q$, where

$$\theta = \sum_{k=0}^{f-1}(r(\varepsilon p^k) - 1)\sigma_{p^k}^{-1},$$

$q = p^f = |\mathbf{F}_{\mathfrak{p}}|$ and $\mathbf{F}_{\mathfrak{p}}$ is the residue field at $\mathfrak{p}$. For $t \in \mathbf{Z}_m^*$ set $s(t) = r(\varepsilon t)^{-1} - 1$. Then if $x \in \mathcal{O}_{\mathfrak{p}}^*$,

$$x^{\theta} \equiv x^{\alpha} \mod \mathfrak{p}$$

where $\alpha = \sum_{k=0;s(p^k)=1}^{f-1} p^k$ and if $y \in \mathcal{O}_{\mathfrak{p}}$ and $x = 1 + py$

$$x^{\theta} \equiv 1 + \left(\sum_{\substack{k=0\\ s(p^k)=1}}^{f-1} y^{p^k}\right) p \mod \mathfrak{p}^2.$$

Now $0 < \alpha < q-1$ unless $p=2$ and $s(p^k)=1$ for all $0 \le k < f$, i.e., unless $p=2$ and

$$\Phi_{a,b,c}\sigma_2 = \Phi_{a,b,c}. \tag{1}$$

As in [G-K] this means $J^{\text{new}}_{a,b,c}$ is ordinary at 2. Hence if $p>2$ or $J^{\text{new}}_{a,b,c}$ is not ordinary at 2 there exists an $x \in \mathscr{O}^*_{\mathfrak{p}}$ such that $x^\theta \not\equiv 1 \mod \mathfrak{p}$. Hence if $\operatorname{order}(Q) = \mathfrak{p}$, Q is not fixed by $A(x)$ which implies (i′).

Also, if

$$f(T) = \sum_{\substack{k=0 \\ s(p^k)=1}}^{f-1} T^{p^k}$$

then $\deg f(T) \le p^{f-1} < q$, so there exists a $y \in \mathscr{O}_{\mathfrak{p}}$ such that

$$(1+py)^\theta \not\equiv 1 \mod \mathfrak{p}^2.$$

It follows that if $\operatorname{order}(Q) = \mathfrak{p}^2$ then Q is not fixed by $A(y)$. This yields (ii′), and so completes the proof of the proposition.

Now $J^m_{a,b,c}$ is isogenous to $\prod_{d|m}(J^d_{a,b,c})^{\text{new}}$, and the degree of the isogeny divides a power of m. Since $J^m_{a,b,c}$ has good reduction outside m, we deduce from Propositions 5, 6 and 10:

Proposition 12. *Suppose p is a rational prime not dividing m such that p divides the exponent of $T^m_{a,b,c}$. Then one of the following holds:*

(i) *$p=2$ and $F^m_{a,b,c}$ is hyperelliptic.*

(ii) *$p=2$, $F^m_{a,b,c}$ is not hyperelliptic, 4 does not divide the exponent of $T^m_{a,b,c}$ and there exists a d dividing m such that $(J^d_{a,b,c})^{\text{new}}$ has positive dimension and is ordinary at 2.*

(iii) *$p=3$, 9 does not divide the exponent of $T_{a,b,c}$, and $F^m_{a,b,c}$ is ordinary at 3.*

VI. Ordinary reduction of Fermat Jacobians

Fix m, a, b, c as always except that we now allow $g_{a,b,c} = 1$.

Proposition 13. *Suppose $(m, 6p) = 1$. Then $J^{\text{new}}_{a,b,c}$ has ordinary reduction at p iff one of the following holds:*

(i) *$p \equiv 1 \mod m$ or*

(ii) *$p^2 \equiv 1 \mod m$ and $(a,b,c) \sim (1, p, -(1+p))$,*

(iii) *$1+p+p^2 \equiv 0 \mod m$ and $(a,b,c) \sim (1, p, -(1+p))$.*

Remarks. (a) Conditions (ii) and (iii) imply that $H_{a,b,c}$ is normalized by an automorphism of $F_{a,b,c}$ obtained from a permutation of $\{X, Y, Z\}$ of order two in the first case and of order three in the second. As a consequence, $F_{a,b,c}$ has automorphisms not in $G_{a,b,c}$ over $\mathbf{Q}$ of order 2 or 3 in the respective cases.

(b) By results of Aoki this result can be shown to hold without the hypothesis $(m, 6) = 1$ so long as m is sufficiently large (see [A]).

Proof. We follow the proof of Lemma 2.5 in [G-R]. As in [G-R] we have $J_{a,b,c}$ is ordinary at p iff

$$\Phi_{a,b,c}\sigma_p = \Phi_{a,b,c}.$$

As $\Phi_{a,b,c}\sigma_p^{-1} = \Phi_{pa,pb,pc}$ Theorem 1 of [K-R] implies, under the hypothesis $(m, 6) = 1$, that $\{a, b, c\} \equiv \{pa, pb, pc\} \bmod m$. Hence one of the following sets of congruences mod m holds:

(a) $a \equiv pa$, $b \equiv pb$, $c \equiv pc$,

(b) $a \equiv pb$, $b \equiv pa$, $c \equiv c$,

(c) $a \equiv pb$, $b \equiv pa$, $c \equiv pa$.

Now (a) implies $p \equiv 1 \bmod m$ as $(m, a, b, c) = 1$, while (b) implies $(a, m) = (b, m) = 1$, $p^2 \equiv 1 \bmod m$ and $p \equiv 1 \bmod m/(m, c)$. If $a \equiv b \bmod m$ then $p \equiv 1 \bmod m$. Otherwise $(a, b, c) \sim (1, p, -(1+p))$. Statement (iii) follows similarly.

(Note: We have just repeated the proof of Theorem 2 of [K-R] in a special case.)

Corollary 13.1. *Suppose* $(m, 6) = 1$.

(i) $J^{\text{new}}_{a,b,c}$ *is ordinary at* 2 *iff* $m = 7$ *and* $(a, b, c) \sim (1, 2, -3)$.

(ii) $J^{\text{new}}_{a,b,c}$ *is ordinary at* 3 *iff* $m = 13$ *and* $(a, b, c) \sim (1, 3, -4)$.

In particular:

Corollary 13.2. *Suppose* $(m, 6) = 1$, *then* $F_{a,b,c}$ *is ordinary at* 3 *iff* $m = 13$ *and* $(a, b, c) \sim (1, 3, -4)$.

Remark. $(J^{15}_{1,2,-3})^{\text{new}}$ is ordinary at 2.

We will now prove

Lemma 14. *Suppose* $(m, 3) = 1$. *Then* $F_{a,b,c}$ *has ordinary reduction at* 3 *iff* m *is either* 8 *or* 13 *and* $(a, b, c) \sim (1, 3, -4)$.

Proof. First note that $F_{a,b,c}$ is ordinary at p iff $(J^d_{a,b,c})^{\text{new}}$ is ordinary at p for all d dividing m, iff

$$\Phi^d_{a,b,c}\sigma_p = \Phi^d_{a,b,c}$$

for all d dividing m iff

$$pL''_{a,b} \equiv L''_{a,b} \mod m. \tag{1}$$

From this we see that $F_{a,b,c}$ is ordinary, then so is F_d for all d dividing m. (This can also be deduced from general principles.)

By Corollary 13.2 we may suppose $m = 2n$. The lemma will follow by induction from the next two lemmas.

Lemma 15. *Suppose $F^n_{a,b,c}$ has genus zero. Then $F^m_{a,b,c}$ is ordinary at* 3 *iff* $m = 8$ *and* $(a, b, c) \sim (1, 3, -4)$.

Proof. Since $g_{a,b,c} \geq 2$ we may suppose $n \geq 4$. Also, after a permutation of $\{a, b, c\}$ we may suppose n divides b and $(a, m) = 1$. Then

$$L''_{a,b} = \{(i, n): 0 < i < n, (i, 2) = 1\}.$$

Let $n = 3k + i$, $0 < i < 3$. Let $j = 1$ if k is even and $j = 2$ if k is odd. Then $(k + j, n) \in L''_{a,b}$ but $3(k + j, n) = (3j - i + n, n) \bmod m$ which lies in $L'_{a,b} - L''_{a,b}$ unless $3j - i > n$. This inequality implies $j = 2$ so that $n = 4$ or 5, but if $n = 5$, $i = 2$ and $3j - i = 4 < n$. Hence $n = 4$, and as $(1, 4) \in L_{a,b}$,

$$(a, b, c) \sim (1, 4, -5) \underset{n}{\sim} (1, 3, -4).$$

As $3L_{1,4} \equiv L_{1,4} \bmod 8$, $F_{a,b,c}$ is ordinary at 3. This completes the proof.

Lemma 16. *Suppose* $n = 8$ *or* 13 *and*

$$(a, b, c) \underset{n}{\sim} (1, 3, -4). \tag{2}$$

Then $F^m_{a,b,c}$ is not ordinary at 3.

Proof. Case (i): $n = 8$. Then one checks that (2) implies

$$(a, b, c) \underset{m}{\sim} (1, 3, -4)$$

but $(3, 9) \in L''_{a,b}$ while $3(3, 9) \equiv (9, 11) \bmod 16$ which lies in $L'_{a,b} - L''_{a,b}$.

Case (ii): $n = 13$. Then one checks that (2) implies

$$(a, b, c) \underset{m}{\sim} (1, 3, -4)$$

but $(5, 15) \in L''_{a,b}$ while $3(5, 15) = (15, 19) \bmod 26$ which lies in $L'_{a,b} = L''_{a,b}$. This completes the proof.

Theorem 9 will now follow from Propositions 12 and 13 together with the following two lemmas.

Lemma 17. $T^{13}_{1,3,-4} = C^{13}_{1,3,-4}$.

Lemma 18. *The extension $\mathbf{Q}(T^8_{1,3,-4})/\mathbf{Q}$ is unramified above* 3.

Proof of Lemma 17. Set $m = 13$ and $F = F^{13}_{1,3,-4}$. Let $\tau \in \mathrm{Aut}(F)$ be defined by $\tau: (X, Y, Z) \mapsto (Z, Y, X)$. Then

$$\tau H_{a,b,c} \tau^{-1} = H_{3,-4,1} = H_{1,3,-4}.$$

It follows that τ descends to an automorphism of F. (See remark after Proposition 13.) We still call this automorphism τ. Then τ and $G_{1,3,-4}$ generate a nonabelian group, G, of order 39. let $p = 3$ and let $\mathfrak{p}$ be some prime above 3 of $\overline{\mathbf{Q}}$ and extend scalars to K via $\mathfrak{p}$ without changing notation. Then if U is a residue class of F which contains a point of T not in $F(K)$ then it follows from Proposition 15(iii) of [C-3] that $\#(U \cap T_{1,3,-4} - U(K)) = 2$ and in the notation of §4 of [C-1] or §3 of [C-2] that

$$\mathbf{P}(\mathscr{C})(j(U)) = j(U), \tag{3}$$

where $j: \widetilde{F} \to \mathbf{P}(W_{1,3,-4})$ is the canonical embedding and $\mathscr{C}$ is the Cartier operator. An easy computation reveals that

$$\mathscr{C}: \begin{array}{ccccccc} \widetilde{\nu}_{1,3} & \mapsto & \widetilde{\nu}_{4,1} & \mapsto & \widetilde{\nu}_{3,9} & \mapsto & \widetilde{\nu}_{1,3}, \\ \widetilde{\nu}_{2,6} & \mapsto & \widetilde{\nu}_{5,2} & \mapsto & \widetilde{\nu}_{6,5} & \mapsto & \widetilde{\nu}_{2,6}. \end{array}$$

From this, it follows easily that $U = (-1, \zeta)$ where $\zeta \in \mu_{13}(\overline{\mathbf{F}}_3)$ in the affine coordinates u and w on F. Hence $T = T_{1,3,-4} - \mathbf{F}(K)$ has at most 26 elements. On the other hand, G preserves T since it preserves $C_{1,3,-4}$ and is defined over $\mathbf{Q}$. It follows that each element of T must be fixed by some element of G. Now the points of F fixed by $G_{1,3,-4}$ are just the cusps, which lie in $F(K)$. Hence, each element of T must be fixed by some subgroup of order 3 of G. By Sylow's theorem these subgroups are all conjugate in G. It follows that if $T \neq C_{1,3,-4}$ then T contains a fixed point Q of τ. Now Q must equal $(-\omega, \omega)$ where ω is a primitive cube root of unity. Then T also contains $\overline{Q}$ (the "complex conjugate" of Q). But if c denotes the cusp at infinity on F, then the divisor class of $Q + \overline{Q} - 2c$ has infinite order as in Theorem 2.1 of [G-R]. This is a contradiction which yields the lemma.

Proof of Lemma 18. Let $F = F^8_{1,3,-4}$. Then with respect to the affine equation $w^8 = u(1-u)^3$, it has the automorphism $\tau: (u, w) \to (1-u, w^3/(1-u))$. This together with $G_{1,3,-4}$ generates a group G of order 16. Since τ stabilizes the cusps, G acts on $T = T^8_{1,3,-4}$. Let S denote the subset of T consisting of points ramified at some prime above 3. Suppose $S \neq \varnothing$. Then G acts on S. The fixed points of τ are $(1/2, \pm 1/\sqrt{2})$. Hence, the set of points fixed by some conjugate of τ is $\{(1/2, \varepsilon/\sqrt{2}),\ \varepsilon \in \mu_8(\overline{\mathbf{Q}})\}$. Since neither these points nor the cusps are ramified above 3, no point in S is fixed by any nontrivial element of G. Hence, if $Q \in S$, $\#GQ = 16$. Now F is ordinary at 11 and has genus 2, so by Theorem A of [C-1], $\#T \leq 22$. Since the number of cusps is 6, it follows that $\#S = 16$ and $S = GQ$ for any $Q \in S$.

Let $E = F/\langle\tau\rangle$. Let $f: F \to E$ denote the natural map. Let O denote the image of (O, O). Then (E, O) is an elliptic curve over $\mathbf{Q}$ with potential CM over $\mathbf{Q}(\sqrt{-2})$ by $\mathbf{Z}[\sqrt{-2}]$. The function field of E over $\mathbf{Q}$ is generated by

$$x = \frac{w^2}{1-u} + \frac{1-u}{w^2} \quad \text{and} \quad y = \frac{1}{w} + \frac{1-u}{w^3}$$

which are related by the equation

$$y^2 = (x^2 - 2)(x + 2). \tag{4}$$

The origin, O, is the point at infinity with respect to this model. It follows that $f(S)$ is a set of eight torsion points on E, stable under $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Claim. $f(S)$ contains a point of the form $P+Q$ where P is a point of order 3 and Q is a point of order 2^n.

We know from Proposition 12 that every point in $f(S)$ has exponent dividing $3\cdot 2^n$ for some $n\in\mathbf{N}$. Since E has good reduction outside 2, all we need show is that $f(S)$ contains a point ramified above 3.

Let $p=3$. Let $\mathfrak{p}$ be a prime of $\overline{\mathbf{Q}}$ above 3. Extend scalars to K via $\mathfrak{p}$. Then each residue class of F which contains one point of S contains exactly two by Proposition 15(iii) of [C-3]. Moreover, these two points are conjugate by $I_{\mathfrak{p}}=\mathrm{Aut}_{\mathrm{cont}}(\mathbf{C}_p/K)=$ inertia group at $\mathfrak{p}$. It follows that S is contained in a set R of 8 residue classes. Moreover, R is stable under G. We know by Proposition 6 that none of these residue classes contains a cusp. Hence,

$$R=\{(1/2\,,\varepsilon/\sqrt{2})^{\sim}:\varepsilon\in\mu_8(\mathbf{C}_p)\}.$$

In particular, if $U=(1/2\,,\varepsilon/\sqrt{2})^{\sim}$ where $\varepsilon^2=-1$ then U is not fixed by τ. Thus if $\{x\,,x'\}=U\cap S$, $f(x)\neq f(x')$; but these two points are conjugate by $I_{\mathfrak{p}}$, hence they are ramified at p. This establishes the claim.

Let $E_3=E[3](\overline{\mathbf{Q}})-\{0\}$. We observe that by the theory of CM elliptic curves, $\mathbf{Q}(E_3)$ is a Galois extension of $\mathbf{Q}$ whose Galois group is dihedral of order 8 and whose quadratic subfields are

$$\mathbf{Q}(\sqrt{-2})\,,\quad \mathbf{Q}(\sqrt{-3})\,,\quad \mathbf{Q}(\sqrt{6})\,. \tag{5}$$

In particular, the eight points in E_3 are all conjugate by $G_{\mathbf{Q}}$. Thus $f(S)$ must be the orbit of $P+Q$ under $G_{\mathbf{Q}}$. Let $Q_0=(-2\,,0)$ on E with respect to the coordinates x and y. Then Q_0 is a point of order 2.

Claim. If P is a nontrivial point of order 3 on E and Q is a point of 2-power order such that $Q\notin\{0\,,Q_0\}$, then $P+Q$ has at least 16 conjugates.

Without loss of generality, we may assume that either $Q=(\sqrt{2}\,,0)$ or $2Q=Q_0$.

If $Q=(\sqrt{2}\,,0)$, then $P+Q$ has 16 conjugates since $\mathbf{Q}(\sqrt{2})$ is not among the fields in (5) and so in linearly disjoint from $\mathbf{Q}(E_3)$.

If $2Q=Q_0$, then $\mathbf{Q}(Q)$ is an extension of $\mathbf{Q}$ of degree at most 2 unramified outside 2. Hence it is distinct from the fields $\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{6})$. Next we observe that $\#E(\mathbf{F}_3)=2$ so that $\mathbf{Q}(Q)\subsetneq\mathbf{Q}(\sqrt{-2})$. Again it follows that $P+Q$ has 16 conjugates. This establishes the claim.

We now see that $f(S)=E_3$ or E_3+Q_0. By computing inflection points we see that $A\in E_3$ iff $x(A)$ is a root of

$$h(T)=3T^4+8T^3+2T^2-48T-36.$$

Also, if $B=(x\,,y)+Q_0$ then

$$x(B)=-2(x+1)/(x+2)=L(x).$$

Now let ε be a primitive 8th root of unity and set $i=\varepsilon^2$. Then $(u\,,w)\in S$ iff $(u\,,\varepsilon w)\in S$. Let $z=w^2/(1-u)$. Then $z(u\,,iw)=iz$. Let $g(T)=$

$h(T+T^{-1})$ if $f(S) = E_3$ and

$$g(T) = ((T+2)h(L(T))) \circ (T+T^{-1}) \quad \text{if } f(S) = E_3 + Q_0.$$

Then $S = \{A \in F(\overline{\mathbf{Q}}) : g(z(A)) = 0\}$ and also

$$S = \{A \in F(\overline{\mathbf{Q}}) : g(iz(A)) = 0\}.$$

Since $\#S = 16$ it follows that g can have no multiple roots. Hence we must have $g(T) = cg(iT)$ for some $c \in \overline{\mathbf{Q}}$. By inspection we see that this is false. Hence we have reached a contradiction and have proven the lemma.

Remark. Based on the above proof one can show that $\#T = 6$ or 22 and $\#f(T - C_{1,2,-4}) = 0$ or 8. It should now be possible to compute T by considering the inverse image in $F(\overline{\mathbf{Q}})$ of points in $E(Q)$ of 2-power order and at most 8 conjugates. We have not done this.

VII. Unbranched Abelian covers of $\mathbf{P}^1 - \{0, 1, \infty\}$

Let m, a, b, c be as always and $f_{a,b,c} : F_m \to F_{a,b,c}$ be as in §II.

Proposition 22. *Suppose p is a rational prime not dividing m and $\mathbf{Q}(T_{a,b,c})/\mathbf{Q}$ is unramified above p. Then $f_{a,b,c}^{-1}(T_{a,b,c})$ is unramified above p.*

Proof. Let $\mathfrak{p}$ be a rational prime of $\overline{\mathbf{Q}}$ above p. Extending scalars to the ring of integers of K via $\mathfrak{p}$, $f_{a,b,c}$ is cyclic and étale outside $u^{-1}\{0, 1, \infty\}$. It follows that if $Q \in T_{a,b,c}$ such that $\tilde{u}(\widetilde{Q}) \notin \{0, 1, \infty\}$ then $f_{a,b,c}^{-1}(Q) \subseteq F_m(K)$. Hence $\mathbf{Q}(f_{a,b,c}^{-1}(Q))/\mathbf{Q}$ is unramified at $\mathfrak{p}$.

On the other hand, if $\tilde{u}(\widetilde{Q}) \in \{0, 1, \infty\}$ then it follows from Proposition 6 that $u(Q) \in \{0, 1, \infty\}$ so that $\mathbf{Q}(f_{a,b,c}^{-1}(Q)) \subseteq \mathbf{Q}(\mu_{2m})$. As $\mathbf{Q}(\mu_{2m})/\mathbf{Q}$ is unramified above p, this completes the proof.

Theorem 23. *Suppose $f : X \to \mathbf{P}^1_{\mathbf{Q}(\mu_m)}$ is an Abelian covering of curves of exponent m unbranched outside $\{0, 1, \infty\}$ of genus at least 2. Then $f^{-1}\{0, 1, \infty\}$ is contained in a torsion packet T such that $\mathbf{Q}(T)/\mathbf{Q}$ is unramified outside m unless X is hyperelliptic, in which case it is unramified outside $2m$.*

Proof. First we observe that the maximal Abelian covering of $\mathbf{P}^1_{\mathbf{Q}(\mu_m)}$ of exponent m unramified outside $\{0, 1, \infty\}$ is $F_m \xrightarrow{u} \mathbf{P}^1_{\mathbf{Q}(\mu_{2m})}$. The Galois group of this covering is $G_m(\overline{\mathbf{Q}})$ which is a product of two cyclic groups of order m. Hence $X \cong F_m/H$ over $\mathbf{Q}(\mu_{2m})$ for some cyclic subgroup of G_m. The order of this subgroup divides m. If $\#H = m$ then $H = H_{a,b,c}$ for some integers a, b and c such that $(m, a, b, c) = 1$ and $a + b + c = 0$. Hence, in this case, the result follows from Theorem 9. Thus we may assume $\#H = d$ for some $d < m$. If $m = 4$ or 5 then $d = 1$ since $g(X) > 1$, and the result follows from Theorem A of [C-2]. We may now suppose that $m > 5$. It suffices, by

Propositions 22 and 13, to show that $H \subseteq H_{a,b,c}$ for some integers a, b, c satisfying

$$(*) \qquad a+b+c=0, \quad (m, a, b, c)=1$$

and

$$(**) \qquad m \text{ does not divide } a, b \text{ or } c$$

if m is even. If m is odd we must find a, b, c as above such that

$$(***) \qquad (a, b, c) \not\sim (1, 1, -2)$$

by Proposition 8. (Note: This will imply X is not hyperelliptic in this case.)

Let $l = m/d$ so that $l \geq 2$. By replacing H with a larger cyclic subgroup of G_m we may suppose l is prime. Clearly $H \subseteq H_{a,b,c}$ for some a, b, c satisfying $(*)$. Let $r, s, t \in \mathbf{Z}$ such that $r+s+t=0$. Set $a' = a - rd$, $b' = b - sd$, and $c' = c - td$. Then $a' + b' + c' = 0$ and $H \subseteq H_{a',b',c'}$. Moreover, $(m, a', b', c') = 1$ iff $a \not\equiv rd \bmod l$ or $b' \not\equiv sd \bmod l$. Also a', b', c' satisfy $(**)$ if

$$a \not\equiv rd \bmod m, \quad b \not\equiv sd \bmod m, \quad c \not\equiv td \bmod m$$

and $m > 6$. If $m = 6$ we must have in addition that $a'b'c' \not\equiv 0 \bmod 6$. Suppose for the moment that $m > 6$. If $g_{a,b,c} = 0$ then by symmetry we may suppose that m divides a and $(m, b) = (m, c) = 1$. It follows that m does not divide $a' = a - d$, $b' = b$ or $c' = c + d$. This completes the proof for even m greater than 6.

Now suppose m is odd and $m > 6$. As above we can find a', b', c' satisfying $(*)$ and $(**)$. Suppose they do not satisfy $(***)$. Then we may suppose $(a', b', c') = (1, 1, -2)$. Replacing a, b and c with $(1-d, 1, d-2)$ we obtain the desired result for odd m.

Finally, the case of $m = 6$ can be handled by inspection.

Theorem A of the Introduction follows from this and Theorem 9, since the natural map of the Jacobian of X into $\prod_{a,b,c} J^m_{a,b,c}$ has a finite kernel of order dividing a power of m.

VIII. Klein's twisted quartic

Let $F = F^7_{1,2,-3}$. Then up to a projective transformation, the canonical embedding of F in $\mathbf{P}^2_{\mathbf{Q}}$ has the equation

$$(1) \qquad X^3Y + Y^3Z + Z^3X = 0,$$

which is the equation of the well-known curve of genus 3 studied by Klein [K] with 168 automorphism. The map is given by $(u, w) \to (u-1, w^3, w(u-1))$. The curve F is also the unique cyclic Fermat quotient of positive genus ordinary at 2. This can be verified by an argument similar to the proof of Lemma 15. Also F is not hyperelliptic and is ordinary at 11. Hence by Theorem A of [C-1], if $T = T_{1,2,-3}$, $\#T \leq 33$. Now, as in the proof of Lemma 17, the automorphism $(X, Y, Z) \mapsto (Y, Z, X)$ of F normalizes $H_{1,2,-3}$ and so induces an automorphism τ of F of order 3. Moreover τ and $G_{1,2,-3}$ generate a nonabelian group G of order 21. (Note: The existence and form of τ is evident from (1).) The fixed points of τ are $(1, \omega, \omega^2)$, $\omega \in \mu_3$, in X, Y, Z coordinates. Thus every fixed point of a conjugate of τ by an element of G is ramified above 3. It follows from Theorem 9 that no noncuspidal element of T is fixed by any nontrivial element of G.

Let ζ denote a primitive 7th root of unity. Then the point

$$P = (\zeta - \zeta^{-1}, \zeta^2 - \zeta^{-2}, \zeta^4 - \zeta^{-4})$$

in $\mathbf{P}^2(\mathbf{Q}(\mu_7))$ lies on the curve cut out by (1). By [F] (see also [G-R, §4]) the rank of the Mordell-Weil group of F over $\mathbf{Q}(\mu_7)$ is zero. Hence $P \in T$. Since P is not a cusp it follows by the above remark that P is not fixed by any element of G. Hence $\#GP = 21$. Thus T contains the 24-element set $W = C_{1,2,-3} \cup GP$. Moreover, as we observed earlier, if $Q \in T - W$ then $\#GQ = 21$. As $21 + 24 > 33$, $T = W$.

For $i \in \{0, 1, \infty\}$, let $c_i = u^{-1}(i)$. Prappavessi has checked that the divisor class represented by

$$P + \tau P + \tau P^2 - (c_0 + c_1 + c_\infty)$$

has order 2. Hence 2 divides the exponent of the divisor class of $P - c$. By Theorem 9, this exponent is of the form $2 \cdot 7^n$. By [G] we must have $n \leq 1$. Since F is not hyperelliptic, we must have $n = 1$. We have proven:

Proposition 24. *The cuspidal torsion packet on the Klein curve has order* 24 *and exponent* 14.

Remark. Compare this result with the example at the end of [C-2] and with Greenberg [G]. Prappavessi has also shown the group of divisor classes supported on T is $J_{1,2,-3}(\mathbf{Q}(\mu_7))$.

Also note that this is a counterexample to Theorem 5.3 of [C-1]. As one can easily verify, the fourth sentence of the proof of this theorem is true only when $p > 2$.

It is not difficult to check that the elements in W are Weierstrass points. Since 24 is the maximum number of Weierstrass points on a curve of genus 3, W is the complete set of Weierstrass points on F.

From this and the fact that the rank of the Mordell-Weil group is zero we deduce

Corollary 24.1. $F(\mathbf{Q}(\mu_7)) = W$ *and is the set of Weierstrass points.*

This implies

Corollary 24.2 (Hurwitz [H]). *$F(\mathbf{Q})$ is the set of cusps.*

Next we prove that Klein's twisted quartic is the only curve of genus 3 over $\mathbf{C}$, up to isomorphism, with 168 automorphisms.

Lemma 25. *Suppose C is a curve over $\mathbf{C}$ of positive genus g with an automorphism of prime order $p > \max(2, g)$. Then C is isomorphic to $F^p_{a,b,c}$ for some $a, b, c \in \mathbf{Z}$ such that $a+b+c=0$ and $(p, a) = (p, b) = (p, c) = 1$.*

Proof. Apply the Riemann-Hurwitz formula.

Corollary 25.1. (i) *Let C be a curve of genus 3 over $\mathbf{C}$ with an automorphism of order 7. Then C is isomorphic to $F^7_{1,1,-2}$ or $F^7_{1,2,-3}$.*

(ii) *In the first case the automorphism group of C is cyclic of order 14. In the second it is isomorphic to $\mathrm{PSL}_2(\mathbf{F}_7) \cong \mathrm{GL}_2(\mathbf{F}_7)$, and so has order 168.*

Proof. Assertion (i) follows immediately from the lemma.

Let G denote the automorphism group of C. If $C = F^7_{1,1,-2}$ then C is hyperelliptic, and if ρ denotes the hyperelliptic involution then ρ is in the center of G. Hence $G/\langle\rho\rangle$ acts on $C/\langle\rho\rangle = \mathbf{P}^1$ and must preserve the 8 branch points, corresponding to $w = \infty$ or $u = \frac{1}{2}$. It is easy to see that the subgroup preserving these points has order 7. This takes care of the first case.

Now suppose $C = F^7_{1,1,-3}$. To show that $G \cong \mathrm{PSL}_2(\mathbf{F}_7)$ it suffices to show, after Hurwitz's Theorem that $\#G \leq 168$ and Lemma 25, that there exists a curve of genus 3 over C on which $\mathrm{PSL}_2(\mathbf{F}_7)$ acts nontrivially. For this, first observe that $\mathrm{PSL}_2(\mathbf{F}_7)$ is generated by three elements σ, τ, ρ satisfying

$$\sigma\tau\rho = \sigma^7 = \tau^3 = \rho^2 = 1.$$

Hence by the Riemann Existence Theorem, there exists a normal covering $X \to \mathbf{P}^1_{\mathbf{C}}$ with Galois group $\mathrm{PSL}_2(\mathbf{F}_7)$, unbranched outside 0, 1 and ∞, with ramification indices 7, 3 and 2 respectively. Using the Riemann-Hurwitz formula, again we see that the genus of C is 3, as required.

It is now possible, as Klein [K] does, to compute explicitly the other automorphisms of (1). We will give a somewhat simpler computation of these automorphisms than Klein's.

Identify F with the hypersurface in $\mathbf{P}^2_{\mathbf{C}}$ cut out by (1). Since this is the canonical embedding of F, the automorphisms of F over $\overline{\mathbf{Q}}$ extend to projective transformations of $\mathbf{P}^2_{\mathbf{C}}$.

To compute the automorphism group, it will suffice to find an automorphism ρ of order 2 normalizing $\langle\tau\rangle$, since this element τ, and $G^7_{1,2,-3}$ must generate the automorphism group of F. As $\rho\tau\rho = \tau^{-1}$, it follows that ρ is represented by a matrix of the form

$$\begin{pmatrix} A & B & C \\ B & C & A \\ C & A & B \end{pmatrix}.$$

Now the Weierstrass points of F are preserved by the automorphisms of F. Hence $\rho(1, 0, 0) = (A, B, C)$ is a Weierstrass point. Since $\rho^2 = 1$, (A, B, C) is not a cusp. Since τ is defined over $\mathbf{Q}$, the set of automorphisms $S = \{\rho, \rho\tau, \rho\tau^2\}$ is stable under $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Hence (A, B, C) has at most three conjugates. It follows from an inspection of W that

$$(A, B, C) = (\zeta - \zeta^{-1}, \zeta^2 - \zeta^{-2}, \zeta^4 - \zeta^{-4})$$

for some primitive seventh root of unity ζ. These three choices correspond to the three elements of S. This completes the computation.

Concluding Remarks. 1. Theorem B of [C-2] follows from Propositions 10, 12 and 13, together with Theorem A of [C-2], so long as $(m, 3) = 1$. To deduce it for all m, one needs to first determine all $(J^m_{a,b,c})^{\mathrm{new}}$ ordinary at 2.

2. As explained in the remark following Proposition 13, $F^m_{a,b,c}$ sometimes has automorphisms not in $G^m_{a,b,c}$ and hence has quotient curves which are not necessarily Abelian covers of $\mathbf{P}^1$ unbranched outside $\{0, 1, \infty\}$, hence are not dealt with by Theorem A. However, their Jacobians have CM and the methods of this paper should apply to prove Conjecture B of [C-3] for the torsion packet containing the image of the cusps. We note that these curves and the curves discussed in this paper are the only curves of genus greater than 3 known to exist which have CM Jacobians.

3. Let X be as in Theorem A. One should also be able to get some information on the power of m dividing the exponent of the cuspidal torsion packet by studying p-adic integrals of the first kind on X for p dividing m. The knowledge of the stable models for $F_{a,b,c}$ [C-M] should be useful for this analysis.

4. It would be interesting to prove Conjecture B of [C-3] for the cuspidal torsion packets on modular curves. We note that $X_1(13)$ has genus 2 and so the conjecture is valid for it, e.g., the cuspidal torsion packet on $X_1(13)$ is unramified outside $2 \cdot 3 \cdot 13$ (13 is the unique prime of bad reduction). On the other hand, one can deduce from the discussion at the end of §6 of [C-1] that this packet is, in fact, ramified above 2, 3 and 13.

References

[A] N. Aoki, *Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves* (to appear).

[C-1] R. Coleman, *Torsion points on curves and p-adic Abelian integrals*, Ann. of Math. **121** (1985), 111–168.

[C-2] ——, *Torsion points on Fermat curves*, Compositio Math. **58** (1986), 191–208.

[C-3] ——, *Ramified torsion points on curves*, Duke J. Math. **54** (1987), 615–640.

[CM] R. Coleman and B. McCallum, *Stable reduction of Fermat curves and Jacobian sum Hecke characters*, J. Reine Angew. Math. **385**, 41–107.

[F] D. K. Faddeev, *On the divisor class groups of some algebraic curves*, Dokl. Akad. Nauk SSSR **136** (1961), 296–298 [Soviet Math. Dokl. **2** (1961), 67–69].

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

[G-R] B. Gross and D. Rohrlich, *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Invent. Math. **44** (1978), 201–224.

[H] A. Hurwitz, *Über die diophantische Gleichang* $x^3y + y^3z + z^3x = 0$, Math. Ann. **65** (1908), 428–430; reprinted in Mathematische Werke II, Birkhäuser-Verlag, Basel and Stuttgart, 1963, pp. 427–429.

[K] F. Klein, *Über die transformation siebenter ordhang der elliptishen funktionen*, LXXXIV Gessammette Mathematische Abhandlungen III, Springer, Berlin, 1923.

[K-R] R. Koblitz and D. Rohrlich, *Simple factors in the Jacobian of a Fermat curve*, Canad. J. Math. **20** (1978), 1183–1205.

[R-2] M. Raynaud, *Courbes sur une variété abelienne et points de torsion*, Invent. Math. **71** (1983), 207–233.

[Ro] D. Rohrlich, *Points at infinity on the Fermat curves*, Invent. Math. **39** (1977), 95–127.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720