COMPOSITIO MATHEMATICA

ROBERT F. COLEMAN

Torsion points on fermat curves

Compositio Mathematica, tome 58, nº 2 (1986), p. 191-208
<http://www.numdam.org/item?id=CM_1986__58_2_191_0>

Compositio Mathematica 58 (1986) 191–208

TORSION POINTS ON FERMAT CURVES

Robert F. Coleman

I. Introduction

Let K be an algebraically closed field of characteristic zero, let m be a positive integer, and let F_m denote the complete plane curve over K with projective equation

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

This is called the Fermat curve of degree m over K. The points in $F_m(K)$ at which one of the projective coordinates vanishes are called the cusps of F_m and the set of such points is denoted by C_m.

It is well known [Ro] and not difficult to show that the difference of any two cusps is a torsion point of order m on the Jacobian of F_m. Using the integration theory we developed in [C], we will show, in Section III,

THEOREM A: *Suppose $m \geqslant 4$ is an integer of the form $\frac{p-1}{n}$ where p is a prime and $1 \leqslant n \leqslant 8$. Suppose P, $Q \in F_M(K)$, P is a cusp and the difference of P and Q is a torsion point on the Jacobian of F_m. Then Q is a cusp.*

We will now introduce some convenient terminology. Let C be a curve over K. Suppose P, $Q \in C(K)$; we write $P \sim Q$ if some integral multiple of the divisor $(P)-(Q)$ is principal. Clearly "$\sim$" is an equivalence relation on $C(K)$. We call an equivalent class of "$\sim$" a torsion packet. A recent theorem of Raynaud [R] asserts that each torsion packet on C is finite when the genus of C is at least two. Via Abel's addition theorem, Theorem A translates into

THEOREM A′: *Suppose m is as in Theorem A. Then C_m is a torsion packet.*

As mentioned in [C], we can show that C_m is the only non-trivial torsion packet when $m+1$ is prime and $m \geqslant 10$. We will not give the proof in this paper. It is similar to that of Theorem A only more complicated.

Call the torsion packet containing C_m the cuspidal torsion packet. Theorem A is proven using rigid analysis at the prime $nm+1$. Using analysis at all primes not dividing m we can prove:

THEOREM B: *Suppose P, Q are in the cuspidal torsion packet of F_m. Then there exists an integer $n>0$ such that $m^n((P)-(Q))$ is principal.*

We can also prove the analogous result for the quotients of F_m (see [G-R]). We will not give the proof of Theorem B here either.

NOTATION: Throughout this paper, p will denote a fixed rational prime, $\mathbb{Z}_p$ the ring of p-adic numbers, $\mathbb{Q}_p$ the field of p-adic numbers, $\mathbb{C}_p$ the completion of a fixed algebraic closure of $\mathbb{Q}_p$, and $\mathbb{R}_p$ the ring of integers in $\mathbb{C}_p$. We will also let $|\ |$ denote a fixed absolute value on $\mathbb{C}_p$. For a field K we will let K^a denote a choice of an algebraic closure of K. For any notation concerning affinoides, see [C], section I.

We would like to thank Joe Buhler for checking our original computations and extending them by computer.

II. Fermat curves

Fix a positive integer m and a prime p not dividing m. Let F_m denote the plane projective curve over $\mathbb{Z}_p$ given by the equation

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

Let F'_m denote the affine open subscheme of F_m consisting of the points at which Z does not vanish. If we set $x=X/Z$, $y=Y/Z$, then x and y are functions on F'_m and

$$F'_m=\operatorname{Spec}\left(\frac{\mathbb{Z}_p[x,y]}{(x^m+y^m+1)}\right).$$

For positive integers a and b, let

$$\omega_{a,b}=x^ay^b\frac{x}{y}\,\mathrm{d}\frac{y}{x}=x^ay^{b-1}\,\mathrm{d}y-x^{a-1}y^b\,\mathrm{d}x,\qquad \omega=\omega_{0,0},$$

be elements of $\Omega^1_{F_m/\mathbb{Z}_p}(F'_m)$. It is easy to see that $\omega_{a,b}$ is a differential of the first kind, i.e. extends uniquely to a global section of $\Omega^1_{F_m/\mathbb{Z}_p}$, if $0<a$, b, $a+b<m$. In fact, these $\dfrac{(m-1)(m-2)}{2}$ diferentials form a basis of $H^0(F_m,\omega^1_{F_m/\mathbb{Z}_p})$ over $\mathbb{Z}_p$.

The subset, $F'_m(\mathbb{R}_p)$, of $F_m(\mathbb{C}_p)$ can naturally be identified with $X(\mathbb{C}_p)$ where X is the affinoide over $\mathbb{Q}_p$ whose coordinate ring $A(X)$ is

$$\frac{\mathbb{Q}_p\langle\langle x,y\rangle\rangle}{(x^m+y^m+1)}.$$

Moreover,

$$A_0(X) = \frac{\mathbb{Z}_p\langle\langle x, y\rangle\rangle}{(x^m + y^m + 1)}$$

the p-adic completion of $\mathcal{O}_{F_m}(F'_m)$ and so $\tilde{X}$ is naturally isomorphic to $\tilde{F}'_m$. In addition, $F_m(\mathbb{C}_p) - X(\mathbb{C}_p)$ is the union of the m-residue classes where $\tilde{Z}$ vanishes. Since F_m has good reduction, each of these residue classes is conformal to the open unit disk in $\mathbb{C}_p$.

Let

$$T^{1/m} = \sum_{n=0}^{\infty} \binom{\frac{1}{m}}{n} (T-1)^n$$

as a formal series in $T - 1$. Since $p \nmid m$ this series actually lies in $\mathbb{Z}_p[[T-1]]$. Hence $T^{1/m}$ converges on the open unit disk about 1 in $\mathbb{C}_p$. Henceforth we will identify $T^{1/m}$ with the corresponding rigid analytic function on this disk. As

$$\tilde{x}^{pm} + \tilde{y}^{pm} + 1 = 0$$

on $\tilde{F}_m$, it follows that $|x_0^{pm} + y_0^{pm} + 1| < 1$ for $(x_0, y_0) \in X$. Hence the composition of the analytic functions $T^{1/m}$ and $-(x^{pm} + y^{pm})|_X$ is a rigid analytic function, h, on X. That is,

$$h = (-(x^{pm} + y^{pm}))^{1/m} = ((1 + x^m)^p - x^{mp})^{1/m}$$

$$= \sum_{n=0}^{\infty} \binom{\frac{1}{m}}{n} ((1 + x^m)^p - (1 + x^{mp}))^n.$$

In fact, h analytically continues to the larger rigid space (wide open space) whose $\mathbb{C}_p$-valued points satisfy the inequality $|x^{pm}(Q) + y^{pm}(Q) + 1| < 1$, but we will not need this.

Now let ϕ be the rigid endomorphism of X which takes

$$(x_0, y_0) \in X \mapsto \left(\frac{x_0^p}{h(x_0, y_0)}, \frac{y_0^p}{h(x_0, y_0)}\right).$$

It is easy to see that $\tilde{\phi}$: $(\tilde{x}_0, \tilde{y}_0) \mapsto (\tilde{x}_0^p, \tilde{y}_0^p)$. In other words, ϕ is a lifting of Frobenius in the sense of [C], section 1, § II.

We will now see how ϕ acts on the differentials $\omega_{a,b}$. First,

$$\phi^*\omega_{a,b} = ph^{-(a+b)}x^{pa}y^{pb}\omega$$

$$= p\sum_{k=0}^{\infty}\begin{pmatrix}\dfrac{-(a+b)}{m}\\ k\end{pmatrix}p^k g(x^m)^k\omega_{pa,pb}$$

where

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

From the relation $x^m + y^m + 1 = 0$ we derive the identities

$$x^{m-1}\,\mathrm{d}x + y^{m-1}\,\mathrm{d}y = 0,\ \mathrm{d}x = xy^m\omega,\ \mathrm{d}y = -x^m y\omega.$$

From these we obtain

$$\begin{aligned}\mathrm{d}x^k y^l &= kx^{k-1}y^l\,\mathrm{d}x + lx^k y^{l-1}\,\mathrm{d}y\\ &= \left(kx^k y^{l+m} - lx^{k+m}y^l\right)\omega\\ &= \left((k+l)x^k y^{l+m} + lx^k y^l\right)\omega\\ &= -\left(kx^k y^l + (k+l)x^{k+m}y^l\right)\omega.\end{aligned}$$

Hence

$$\begin{aligned}x^{a+mr}y^b\omega = \mathrm{d}\Bigg(x^a y^b \sum_{k=1}^{r}\left(\frac{(-1)^k}{a+b+m(r-k)}\right.\\ \left.\times\prod_{i=1}^{k-1}\left(\frac{a+m(r-i)}{a+b+m(r-i)}\right)\right)x^{m(r-k)}\Bigg)\\ +(-1)^r\prod_{i=1}^{r}\left(\frac{a+m(r-i)}{a+b+m(r-i)}\right)x^a y^b\omega\end{aligned} \tag{1}$$

$$\begin{aligned}x^a y^{b+mr}\omega = \mathrm{d}\Bigg(x^a y^b \sum_{k=1}^{r}\frac{(-1)^{k-1}}{(a+b)+m(r-k)}\\ \times\prod_{i=1}^{k-1}\left(\frac{b+m(r-i)}{a+b+m(r-i)}\right)y^{m(r-k)}\Bigg)\\ +(-1)^r\prod_{i=1}^{r}\frac{b+m(r-i)}{a+b+m(r-i)}x^a y^b\omega.\end{aligned} \tag{2}$$

For a real number r we let $[r]$ denote the greatest integer less than or equal to r, also let $\log_p$ denote the real logarithm to the base p.

LEMMA 1: *Suppose* $(m, p) = 1$. *Then*

$$\operatorname{ord}_p\left(\frac{(t-m)(t-2m)\dots(t-lm)}{s(s-m)\dots(s-lm)}\right) \geqslant -\max_{0\leqslant j\leqslant l} \operatorname{ord}_p(s-jm).$$

PROOF: Let $N = \max_{0\leqslant j\leqslant l}[\operatorname{ord}_p(s-jm)] = \operatorname{ord}_p(s-j_0m)$ and $M = \max_{1\leqslant j\leqslant l}\operatorname{ord}_p(t-jm) = \operatorname{ord}_p(t-j_1m)$ for appropriate $0\leqslant j_0\leqslant l$ and $1\leqslant j_1\leqslant l$. Then for $j\neq j_0$, $\operatorname{ord}_p(s-jm) = \operatorname{ord}_p(j-j_0)$, and so

$$\operatorname{ord}_p\left(\prod_{j=0}^{l}(s-jm)\right) = N + \operatorname{ord}_p(j_0!) + \operatorname{ord}_p((l-j_0)!)$$

$$= N + \sum_{i=1}^{r}\left(\left[\frac{j_0}{p^i}\right] + \left[\frac{l-j_0}{p^i}\right]\right)$$

where $r = [\log_p(l)]$. Similarly,

$$\operatorname{ord}_p\left(\prod_{j=1}^{l}(t-jm)\right) = M + \sum_{i=1}^{r}\left(\left[\frac{j_1-1}{p^i}\right] + \left[\frac{l-j_1}{p^i}\right]\right)$$

$$\geqslant \sum_{i=1}^{r}\left(\left[\frac{j_1-1}{p^i}\right] + \left[\frac{l-j_1}{p^i}\right] + 1\right)$$

as $M \geqslant r$.

The lemma now follows from the elementary inequalities

$$\left[\frac{a+b}{k}\right] \geqslant \left[\frac{a}{k}\right] + \left[\frac{b}{k}\right]$$

$$\left[\frac{a}{k}\right] + \left[\frac{b}{k}\right] + 1 \geqslant \left[\frac{a+b+1}{k}\right],$$

for integers a, b and k with $k \geqslant 2$.

Suppose now $p > m$, $p > 2$ and $a + b < 2m$. Fix integers $i > 0$ and $0 \leqslant r \leqslant i(p-1)$. We claim that

$$\binom{-\frac{(a+b)}{m}}{i} p^i x^{rm} \omega_{pa,pb} = c \cdot \omega_{pa,pb} + \mathrm{d}h \tag{3}$$

for some $c \in \mathbb{Q}$, $h \in \mathbb{Q}[x, y]$ such that

$$\operatorname{ord}_p c \geqslant 1 \quad \text{and} \quad \operatorname{ord}_p h \geqslant 1 \quad \text{when} \quad i \geqslant 2,$$

$$\operatorname{ord}_p c \geqslant 0 \quad \text{and} \quad \operatorname{ord}_p h \geqslant 0 \quad \text{when} \quad i = 1.$$

Indeed, applying formula (1) with a, b replaced by pa, pb we find that

$$x^{rm}\omega_{pa,pb} = \mathrm{d}h_1 + c_1\omega_{pa,pb}, \tag{4}$$

where c_1 and the coefficients of h_1 are essentially of the same form as the expressions in Lemma 1 with $s = pa + pb + m(r-1)$, $t = pa + mr$, and $l = k - 1$, where $1 \leqslant k \leqslant r$. It follows from (1) and Lemma 1 that we can find c and h satisfying (3) as well as

$$\left.\begin{matrix}\operatorname{ord}_p c\\ \operatorname{ord}_p h\end{matrix}\right\} \geqslant i + \operatorname{ord}_p \begin{pmatrix} -\dfrac{a+b}{m} \\ i \end{pmatrix} - \max_{0 \leqslant j \leqslant n} \operatorname{ord}_p(pa + pb + jm)$$

$$\geqslant i + \operatorname{ord}_p \begin{pmatrix} -\dfrac{(a+b)}{m} \\ i \end{pmatrix}$$

$$-\left(1 + \max_{0 \leqslant j \leqslant [\frac{n}{p}]} \operatorname{ord}_p(a + b + jm)\right),$$

where $n = i(p-1) - 1$ (which is 0 when $i = 1$ and 1 when $i = 2$). Now suppose $i \geqslant 3$. Then from the above we have (using $p > m$ and $2m > a + b$),

$$\left.\begin{matrix}\operatorname{ord}_p c\\ \operatorname{ord}_p h\end{matrix}\right\} \geqslant i - \left(1 + \log_p\left(a + b + \frac{nm}{p}\right)\right)$$

$$\geqslant i - \left(1 + \log_p\left((p-1)\left(\frac{2+n}{p}\right)\right)\right)$$

$$\geqslant i - \left(\log_p((p-1)(i(p-1)+1))\right)$$

$$\geqslant \log_p\left(\frac{p^i}{i(p-1)^2 + (p-1)}\right)$$

$$> 0 \quad \text{as} \quad i \geqslant 3.$$

This establishes our claim. Since the degree of $g(x)^i$ is $i(p-1)$, it follows from (3) that for $i \geqslant 2$, $a+b<2m$, $p>m$,

$$\binom{-\frac{(a+b)}{m}}{i} p^i g(x^m)^i \omega_{pa,pb} = c_i \omega_{pa,pb} + \mathrm{d}h_i \tag{5}$$

where $c_i \in \mathbb{Q}$, $h_i \in \mathbb{Q}[x]$, $\operatorname{ord}_p c_i \geqslant 1$ and $\operatorname{ord}_p h_i \geqslant 1$. We claim that this also holds for $i=1$. Indeed,

$$pg(x^m)\omega_{pa,pb} = \left(\sum_{j=1}^{p-1} \binom{p}{j} x^{jm}\right) \omega_{pa,pb} \tag{6}$$

and

$$\binom{p}{p-j} x^{(p-j)m} \omega_{pa,pb} = e_j \binom{p}{j} x^{jm} \omega_{pa,pb} + \mathrm{d}f_j$$

for $1 \leqslant j \leqslant \frac{p-1}{2}$, where $f_j \in \mathbb{Q}[x]$, $\operatorname{ord}_p f_j \geqslant 1$, and

$$e_j = (-1)^{p-2j} \prod_{k=1}^{p-2j} \left(\frac{pa+mj+m(p-2j-k)}{p(a+b)+mj+m(p-2j-k)} \right)$$

$$\equiv -1 \bmod p.$$

It follows that

$$\binom{p}{j} x^{jm} \omega_{pa,pb} + \binom{p}{p-j} x^{(p-j)m} \omega_{pa,pb} = e_j' x^{jm} \omega_{pa,pb} + \mathrm{d}f_j'$$

where $\operatorname{ord}_p e_j' \geqslant 2$ and $\operatorname{ord} f_j' \geqslant 1$. Now (5) for $i=1$ follows immediately from (3) and (6).

We deduce:

LEMMA 2: *Suppose $p>m$ and a, $b>0$ and $a+b<2m$. Then*

$$\phi^* \omega_{a,b} = c\omega_{pa,pb} + \mathrm{d}h$$

where $h \in A_0(X)$, $c \in \mathbb{Q}_p$, $\operatorname{ord}_p h \geqslant 2$, and $c \equiv p \bmod p^2 \mathbb{Z}_p$.

Fix a, $b > 0$, and suppose $pa = a' + rm$, $pb = b' + sm$, where a', $b' \geqslant 0$ *and* r, $s \geqslant 0$. Then from (1) and (2),

$$\omega_{pa,pb} = \mathrm{d}\left(x^{pa}y^{pb} \sum_{k=1}^{r} \frac{(-1)^k}{p(a+b)-km} \prod_{i=1}^{k-1} \left(\frac{pa-im}{p(a+b)-im} \right) x^{-km} \right)$$

$$+(-1)^r \prod_{i=1}^{r} \left(\frac{pa-im}{p(a+b)-im} \right) \omega_{a',pb} \tag{7}$$

$$\omega_{a',pb} = \mathrm{d}\left(-x^{a'}y^{pb} \sum_{k=1}^{s} \frac{(-1)^k}{a'+pb-km} \prod_{i=1}^{k-1} \left(\frac{pb-im}{a'+pb-im} \right) y^{-km} \right)$$

$$+(-1)^s \prod_{i=1}^{s} \left(\frac{pb-im}{a'+pb-im} \right) \omega_{a',b'}. \tag{8}$$

If $0 < a$, $b < m$ then $0 \leqslant r$, $s < p$, and so formula (7) implies

$$\omega_{pa,pb} = c_1\omega_{a',pb} + \mathrm{d}h_1$$

where $c_1 \in \mathbb{Z}_p$, $h_1 \in \mathbb{Z}_p[x]$ and

$$c_1 \equiv (-1)^r \bmod p$$

$$h_1 \equiv x^{a'}y^{pb} \sum_{k=1}^{r} \frac{(-1)^k}{-km} x^{-km} \bmod p$$

$$\equiv x^{a'}y^{pb} \sum_{k=1}^{r} \frac{(-1)^k n}{k} x^{-km} \bmod p$$

where in the last congruence n is an integer such that $nm \equiv -1 \bmod p$.

To analyze the formula for $\omega_{a',pb}$ we need

LEMMA 3: *Suppose* $0 < a$, a', b, $b' < m$, *are as above and* $1 \leqslant i \leqslant s$ *is an integer such that* $a' \equiv im \bmod p$. *Then* $i = p - r$, $a + b > m$ *and if* $p > m$, $\mathrm{ord}_p(a' + pb - im) = 1$.

PROOF: Adding rm to both sides of the congruence $a' \equiv im \bmod p$, we obtain

$$pa \equiv (i+r)m \bmod p.$$

Hence p divides $i+r$. Now $i+r \leqslant r+s$ and

$$0 \leqslant r = \frac{pa-a'}{m} < p$$

$$0 \leqslant s = \frac{pb-b'}{m} < p$$

since $0 < a,\ a',\ b,\ b' < m$. Hence for p to divide $i+r$ we must have $i = p - r$. Since $i \leqslant s$ we have $p \leqslant r+s$ and $pm \leqslant rm + ms$, so

$$pm + a' + b' \leqslant pa + pb$$

and

$$m < m + \frac{a'+b'}{p} \leqslant a + b.$$

Finally, with $i = p - r$, we have

$$a' + pb - im = a' + pb - (p-r)m = p(a+b-m).$$

If $p > m$ then p does not divide $a+b-m$ as $1 < a+b-m < m$.

Suppose now, $p > m$ and $0 < a,\ b,\ a',\ b' < m$. From this lemma and (8) it follows that

$$\omega_{a',pb} = c_2 \omega_{a',b'} + \mathrm{d}h_2$$

where

$$\mathrm{ord}_p c_2 = \begin{cases} 0 & \text{if } a+b<m \\ -1 & \text{if } a+b>m \end{cases}$$

$$\mathrm{ord}_p h_2 = \begin{cases} 0 & \text{if } a+b<m \\ -1 & \text{if } a+b>m \end{cases}$$

and where

$$c_2 \equiv (-1)^s \prod_{i=1}^{s} \frac{-im}{a'-im} \bmod p$$

$$\equiv (-1)^s \prod_{i=1}^{s} \frac{i}{r+i} = (-1)^s \binom{r+s}{s}^{-1} \bmod p$$

if $a+b<m$. (Note: here we used the congruence $na' \equiv r \bmod p$. Recall, $nm \equiv -1 \bmod p$.) Similarly we have

$$h_2 \equiv -x^{a'}y^{b'} \sum_{k=1}^{s} \frac{(-1)^k n}{k} \binom{r+k}{k}^{-1} y^{(s-k)m} \bmod pA_0(X)$$

if $a+b<m$,

$$c_2 \equiv (-1)^s \frac{m}{m-(a+b)} \binom{r+s}{s}^{-1} \mod \mathbb{Z}_p$$

$$h_2 \equiv \frac{1}{m-(a+b)} x^{a'} y^{b'} \sum_{k=p-r}^{s} \frac{(-1)^k}{k} \binom{r+k}{k}^{-1} y^{(s-k)m} \mod A_0(X)$$

if $a+b>m$.

Suppose now $p=mn+1$. It follows that $a=a'$, $b=b'$, $r=na$, and $s=nb$.

Let $I=\{(a,b)\in\mathbb{Z}\times\mathbb{Z}: 0<a,\ b<m,\ a+b\neq m\}$,

$I^{1,0}=\{(a,b)\in I: a+b<m\}$,

$I^{0,1}=\{(a,b)\in I; a+b>m\}$.

For $a\in\mathbb{Z}$ let $\hat{a}=m-a$. Combining the above congruences with Lemma 2 we deduce

Proposition 4: *Suppose $(a,b)\in I$. Let $u=-x^m$ and $v=-y^m$. Then*

$$\phi^*\omega_{a,b}=J_{a,b}\omega_{a,b}+p\,\mathrm{d}h_{a,b}$$

where

(i) *If $(a,b)\in I^{1,0}$ then $J_{a,b}\in p\mathbb{Z}_p^*$, $h_{a,b}\in A_0(X)$, and*

$$p^{-1}J_{a,b}\equiv(-1)^{n(a+b)}\binom{n(a+b)}{na}^{-1} \mod p\mathbb{Z}_p,$$

$$h_{a,b}\equiv(-1)^{n(a+b)}nx^ay^b\left(\sum_{k=1}^{na}\frac{1}{k}u^{na-k}v^{nb}-\sum_{k=1}^{nb}\frac{1}{k}\binom{na+k}{na}^{-1}v^{nb-k}\right)$$

$\mod pA_0(X)$.

(ii) *If $(a,b)\in I^{0,1}$, $J_{a,b}\in\mathbb{Z}_p^*$, $h_{a,b}\in(1/p)A_0(X)$ and*

$$p^{-1}J_{a,b}\equiv\frac{(-1)^{n(a+b)}}{n(a+b)+1}\binom{n(a+b)}{na}^{-1}$$

$$\equiv\frac{(-1)^{n(a+b)}}{p}\binom{n(\hat{a}+\hat{b})}{n\hat{a}} \mod \mathbb{Z}_p,$$

$$h_{a,b}\equiv\frac{(-1)^{n(a+b)}}{m-(a+b)}x^ay^b\sum_{k=p-na}^{nb}\frac{1}{k}\binom{na+k}{na}^{-1}v^{nb-k} \mod A_0(X).$$

REMARK: The computations which led to this proposition were fairly complicated. The reader might therefore like to perform some credibility checks. First note that $\tilde{h}_{a,b}$ vanishes at the cusps on X, for each $(a, b) \in I^{1,0}$. This is consistent with the fact that an integral of the first kind is constant on a torsion packet (Proposition 3.1 of [C]). Also it is not difficult (albeit messy) to verify that $\tilde{h}_{a,b} \equiv -\tilde{h}_{b,a}$. This is consistent with the fact that $\omega_{a,b} \leftrightarrow -\omega_{b,a}$ under the automorphism $X \leftrightarrow Y$ of F_m.

III. Integrals modulo p^2

In this section we will give a reformulation of Theorem 4.2 of [C] which is more suitable for computations than the original. We will maintain the notations of [C]. Thus K is the completion of the maximal unramified extension of $\mathbb{Q}_p$ in $\mathbb{C}_p$, $\mathbb{F}$ is the residue field of K and σ denotes the Frobenius automorphism of both K and $\mathbb{F}$. Let R denote the ring of integers of K and let C be a smooth connected curve over R, with generic fiber C_K and special fiber C_0.

Now let V denote a fixed R-submodule of $H^0(C, \Omega^1_{C/R})$ stable under Frobenius in the following sense: Fix a non-empty Zariski affinoide X in C and a lifting ϕ: $X \to X^\sigma$ of absolute Frobenius (see [C], section II) to X. We require

$$\phi^* V^\sigma \subseteq V + \mathrm{d}A(X). \tag{1}$$

It follows that (1) holds for all liftings, ϕ, and all Zariski affinoides X in C.

For $\omega \in V^\sigma$ let $L(\omega)$ denote the unique element of V such that $\phi^*\omega - L(\omega) \in \mathrm{d}A(X)$. The element $L(\omega)$ depends only on ω and not the choice of ϕ or X.

Fix a point $E \in C(K)$. As described in [C], for each $\omega \in V$, there is a canonical locally analytic function λ_ω: $C(\mathbb{C}_p) \to \mathbb{C}_p$ which vanishes at E, satisfies $\mathrm{d}\lambda_\omega = \omega$, and behaves well with respect to Frobenius. In the notation of [C],

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

for all $Q \in C(\mathbb{C}_p)$. Let

$$G_\omega(Q) = \frac{1}{p}\left(\lambda_\omega(\phi(Q)) - \lambda_{L(\omega)}(Q)\right)$$

for $Q \in C(\mathbb{C}_p)$. Then as in Proposition 4.5 of [C], $G_\omega \in A_0(X)$, the ring of integer valued rigid analytic functions on X.

Now suppose U is a residue class of C in X and ϵ is the Teichmüller point of ϕ in U. Let $T \in A_0(X)$ be a local parameter at ϵ such that $\tilde{T}$ is a parameter at U on C_0. Then by equations (17) and (18) in section IV of [C] we have

$$\lambda_\omega(Q) \equiv p(G_{\omega^\sigma}(\epsilon))^{\sigma^{-1}} + \frac{\omega}{dT}(\epsilon)T(Q) \bmod p^2 \tag{2}$$

if $p \geqslant 3$, $Q \in U(\mathbb{C}_p)$ and $|T(Q)| \leqslant |p|$. Since $|T(Q)| \leqslant |p|$ for all $Q \in U(K)$, the following theorem is an immediate consequence of (2).

THEOREM 6: *Let $p \geqslant 3$. Let $\omega_1, \omega_2 \in V$. Suppose $Q \in X(K)$ such that $\tilde{\omega}_1$ does not vanish at $\tilde{Q}$. Then*

$$\int_E^Q \omega_1 \equiv \int_E^Q \omega_2 \equiv 0 \bmod p^2$$

iff

$$\left(G_{\omega_1^\sigma}\left(\frac{\omega_2}{\omega_1}\right)^p - G_{\omega_2^\sigma}\right)^{\sim}(\tilde{Q}) = 0.$$

IV. Torsion points on Fermat curves

We will now apply the results of [C] and the last section to determine the cuspidal torsion packet on F_m for certain m.

Fix $m \geqslant 4$ and $p \equiv 1 \bmod m$. Then the genus of F_m is $\frac{1}{2}(m-1)(m-2) \geqslant 3$ and the Jacobian of F_m is ordinary at p. This follows from the theory of complex multiplication as p splits completely in $\mathbb{Q}(\mu_m)$. As $p > m > 3$ we may apply Theorem A of [C] to conclude T_m is unramified above p.

As in the last section we consider F_m as a curve over $\mathbb{Z}_p$. We let $\tilde{F}_m$ denote the special fiber of F_m over $\mathbb{F}_p$. Since T_m is unramified over p it follows that each residue class of F_m contains at most one element of T_m. In particular, if $c \in C_m$, $c = T_m \cap \tilde{c}$. We call the residue classes $\tilde{c}$, $c \in C_m$, the cuspidal residue classes.

Fix a cusp $c \in F_m - F_m'$. For each $\omega \in H^0(F_m\colon \Omega^1_{F_m/\mathbb{Q}_p})$ set

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

as in [C]. Then by Proposition 3.1 [C], $Q \in T_m$ if and only if

$$\lambda_\omega(Q) = 0 \tag{1}$$

for all $\omega \in H^0(F_m: \Omega^1_{F_m/\mathbf{Q}_p})$. In particular, $\lambda_\omega(Q) = 0$ for all $Q \in C_m$ and so λ_ω does not depend on the choice of E in C_m.

For $(a, b) \in I^{1,0}$ set $\lambda_{a,b} = \lambda_{\omega_{a,b}}$. Now let ϕ and X be as in Section II. From Proposition 4,

$$\phi^* \omega_{a,b} - J_{a,b} \omega_{a,b} \in \mathrm{d}A(X).$$

Hence with notation as in the last section,

$$L(\omega_{a,b}) = J_{a,b} \omega_{a,b}$$

$$G_{\omega_{a,b}} = \frac{1}{p}(\lambda_{a,b} \circ \phi - J_{a,b} \lambda_{a,b}).$$

On the other hand, Proposition 4 implies $h_{a,b} + K = G_{\omega_{a,b}}$ for some constant $K \in \mathbb{Z}_p$.

We claim $K \equiv 0 \bmod p$. First we note that ϕ fixes each element of $C_m \cap X$. Hence as $\lambda_{a,b}$ vanishes on C_m it follows that $G_{\omega_{a,b}}$ vanishes on $C_m \cap X$. Second, it follows from the congruence in Proposition 4 that $\tilde{h}_{a,b}$ vanishes on $\tilde{C}_m \cap \tilde{X}$. The claim is now immediate once we note that $C_m \cap X \neq \emptyset$.

We may now apply Theorem 6 to conclude (noting that the differentials $\omega_{a,b}$, $(a, b) \in I^{1,0}$, vanish only at the cusps):

Proposition 7: *Suppose $(a, b), (a', b') \in I^{1,0}$. Suppose U is a residue class of X not equal to a cusp of $\tilde{F}_m$. Then there exists a point $Q \in U(K)$ such that*

$$\lambda_{a,b}(Q) \equiv \lambda_{a',b'}(Q) \equiv 0 \bmod p^2$$

if and only if

$$\left(h_{a,b}(x^{a'-a} y^{b'-b})^p - h_{a',b'}\right)^{\sim}(U) = 0 \tag{2}$$

Corollary 7a: *Suppose U is a residue class of X not equal to a cusp of $\tilde{F}_m$. Then if U contains an element of T_m the equations* (2) *hold for all (a, b) and (a', b') in $I^{1,0}$.*

Remark: As the cuspidal residue classes already contain elements of T_m and, as mentioned above, each residue class contains at most one, we have only to show that the non-cuspidal classes do not contain elements of T_m in order to show $C_m = T_m$.

We must now compute the functions on the left-hand side of (2). Suppose $(a, b) \in I^{1,0}$ and $b > 1$. It follows easily from Proposition 4 that

$$r_{a,b} \overset{\text{defn}}{=} \frac{1}{n}\left(h_{a,b-1}y^p - h_{a,b}\right)$$

$$\equiv (-1)^{n(a+b)} x^a y^b \sum_{n(b-1)+1}^{nb} \frac{1}{k}\binom{nb+k}{nb}^{-1} v^{na-k}$$

Applying the involution $x \leftrightarrow y$ and noting that $\omega_{a,b} \mapsto -\omega_{b,a}$ under this involution, we deduce that

$$s_{a,b} \overset{\text{defn}}{=} \frac{1}{n}\left(h_{a-1,b}x^p - h_{a,b}\right)$$

$$\equiv -(-1)^{n(a+b)} x^a y^b \sum_{n(a-1)+1}^{na} \frac{1}{k}\binom{nb+k}{nb}^{-1} u^{na-k}$$

for $(a, b) \in I^{1,0}$ with $a > 1$.

We will now determine the common zeros of $r_{a,b}$ and $s_{a',b'}$ for small n.

Case (i): $n = 1$. In this case

$$r_{1,2} = -\tfrac{1}{6}xy^2$$

hence no non-cuspidal residue classes contain elements of T_m. As remarked above, this suffices to conclude that $T_m = C_m$ in this case.

Case (ii): $n = 2$. In this case

$$r_{1,2} = \tfrac{1}{30}xy^2\left(v + \tfrac{1}{2}\right),$$

$$s_{2,1} = -\tfrac{1}{30}x^2y\left(u + \tfrac{1}{2}\right).$$

Hence if the common zeros of $\tilde{r}_{1,2}$ and $\tilde{s}_{2,1}$ include a non-cusp we must have $\tilde{u} = \tilde{v} = -\frac{1}{2}$. We also have $\tilde{u} + \tilde{v} = 1$ and so $-1 = 1$. As $p = 2m + 1 \geqslant 9 > 2$ we conclude again that $T_m = C_m$.

Case (iii): $n = 3$. In this case

$$r_{1,2} = \tfrac{1}{28}\left(\tfrac{1}{5}v^2 + \tfrac{1}{10}v + \tfrac{1}{8}\right)xy^2,$$

$$s_{2,1} = -\tfrac{1}{28}\left(\tfrac{1}{5}u^2 + \tfrac{1}{10}u + \tfrac{1}{8}\right)x^2y.$$

Using $v^2 - u^2 = (v - u)(v + u) = v - u$ we have

$$\frac{r_{1,2}}{xy^2} + \frac{s_{2,1}}{x^2y} = \tfrac{1}{28}\left(\tfrac{1}{5} + \tfrac{1}{10}\right)(v - u) = \tfrac{3}{280}(v - u)$$

so that we must have $v = u = \frac{1}{2}$. But $\frac{1}{5} \cdot \frac{1}{4} + \frac{1}{10} \cdot \frac{1}{2} + \frac{1}{18} = \frac{7}{45}$. We conclude that $C_m = T_m$ in this case as well.

The remaining cases may be handled similarly and Joe Buhler has carried out the computations on computer.

This completes the proof of Theorem A of the Introduction.

REMARK: The smallest m for which we do not yet know whether $T_m = C_m$ is $m = 17$. In this case $n = 6$ is the smallest integer n such that $n \cdot 17 + 1$ is prime.

Fix $m \geqslant 5$. We will now deduce some results about torsion points on the curve

$$F_{1,1}(m)\colon\ w^m = u(1-u).$$

This curve is a hyperelliptic factor of F_m. The map

$$f\colon (x, y) \to (-x^m, xy)$$

takes F_m onto $F_{1,1}(m)$. The map $(u, w) \to (1-u, w)$ is the hyperelliptic involution of $F_{1,1}$.

The hyperelliptic branch points lie in a torsion packet, $T_{1,1}$, which we call the hyperelliptic torsion packet (see [C], §VI). It is not hard to see that this packet contains the images of the cusps on F_m, so that in general $T_{1,1}$ contains at least the set of $2[\frac{m}{2}] + 4$ elements consisting of the cusps and the hyperelliptic branch points. These are the points where $u = 0, \frac{1}{2}, 1$, or ∞.

PROPOSITION 8: *If $m + 1 = p$ is prime, $T_{1,1}$ is exactly the above set of $m + 4$ points.*

PROOF: Using the change of variables formula for integration, Theorem 2.7 of [C], se see that $f(Q) \in T_{1,1}$ for $Q \in F_m(\mathbb{C}_p)$ if and only if

$$\lambda_\omega(Q) = 0$$

for all $\omega \in f^*H^0(F_{1,1}, \Omega_{F_{1,1}/\mathbf{Q}_p})$. It is easy to see that this latter space is spanned by $\{\omega_{i,i}\colon 0 < i < [\frac{m}{2}]\}$.

By Theorem A of [C], each residue class of $T_{1,1}$ contains at most one element of $T_{1,1}$, and this element must lie in $F_{1,1}(K)$. Let U be a residue class of X such that

$$\lambda_{1,1}(Q) \equiv \lambda_{2,2}(Q) \equiv 0 \bmod p^2$$

for som $Q \in U(K)$. By Proposition 7,

$$(h_{1,1}x^p y^p - h_{2,2})^{\tilde{}}(U) = 0.$$

Using Proposition 4 and the hypothesis $p = m + 1$, we see that

$$(h_{1,1}x^p y^p - h_{2,2})^{\tilde{}} = \left(\tfrac{1}{6}x^2y^2\left(u - \tfrac{1}{2}\right)\right)^{\tilde{}}.$$

The proposition follows immediately.

REMARK: As the genus of $F_{1,1}$ is $[\frac{m}{2}] - 1$, this proposition furnishes a sequence of examples where the size of the torsion packet grows proportionately to the genus. On the other hand, the bound given by Theorem A of [C] grows proportionately to the square of the genus in this sequence.

We will now determine the hyperelliptic torsion packet T on the curve C: $w^5 = u(1-u)$. This is the first example not covered by the previous proposition. Let Q_∞ denote the point at infinity on C and let

$$Q_0 = (0, 0),\ Q_1 = (1, 0).$$

Then T contains the three cusps Q_0, Q_1 and Q_∞ as well as the six hyperelliptic branch points where $u = \frac{1}{2}$ or $u = \infty$. Note that Q_∞ is both a cusp and a hyperelliptic branch point. Let H denote this set of eight points. From the previous proposition one might guess that $T = H$. This is not the case.

For now, we will consider C as a curve over $\mathbf{Q}_{11}$. Note that C is ordinary over $\mathbf{Q}_{11}$. Let μ_5 denote the group of 5^{th} roots of unity in $\mathbf{Q}_{11}$. Let K denote the maximal unramified extension of $\mathbf{Q}_{11}$. By Theorem A of [C], $T \subseteq C(K)$ and each residue class contains at most one point of T. As in the proof of Proposition 8, if U is a residue class of $X \subseteq F_m$ whose image in C contains an element of T, then

$$(h_{1,1}x^{11}y^{11} - h_{2,2})^{\tilde{}}$$

vanishes at U (with notation as in Proposition 4, with $p = 11$). Using the congruence in Proposition 4, we obtain

$$(h_{1,1}x^{11}y^{11} - h_{2,2})^{\tilde{}} = \left(\tfrac{2}{10}w^2\left(\tfrac{1}{3}u^2 - u\right) - \tfrac{1}{14}\right)\left(u - \tfrac{1}{2}\right)\big)^{\tilde{}}.$$

(Here we identify w with xy and u with $-x^{11}$.) We conclude that if $U=(u_0, w_0) \in C(\mathbb{F}_{11}^a)$ such that $U \notin \tilde{H}$ and $U \cap T \neq \emptyset$ then

$$\left(u_0^2 - u_0 - 1\right) = (u_0 - 4)(u_0 - 8) = 0$$

and

$$w_0^5 = -1.$$

In particular, $U \in C(\mathbb{F}_{11})$ and $\#(T-H) \leqslant 10$. Now one can show the Jacobian of $\tilde{C}$ has 125 points. Using this and the result of Greenberg [G] one can show that $T-H \subseteq C(\mathbb{Q}(\mu_5)) \subseteq C(\mathbb{Q}_{11})$.

In fact, if $\sqrt{5}$ is a solution of x^2-5 in $\mathbb{Q}_{11}$ then the ten points in $C(\mathbb{Q}(\mu_5))$:

$$\left(\frac{1 \pm \sqrt{5}}{2}, -\xi\right), \ \xi \in \mu_5, \tag{3}$$

all lie in T. Indeed, if $\xi \in \mu_5$ such that $\dfrac{1+\sqrt{5}}{2} = -(\xi^2+\xi^3) \overset{\text{defn}}{=} \alpha$, and $P=(\dfrac{1+\sqrt{5}}{2}, -1)$, then the function

$$\frac{u + w^2 - w^3}{w^4 - \alpha w^3 + w^2}$$

has divisor $\xi P - \xi^2 P - \xi^3 P + \xi^4 P - 2Q_1 + 2Q_\infty$ so that in the Jacobian

$$\sqrt{5}\, P = 2Q_1.$$

Thus $P \in T$. As the other points in (3) are the images of P under automorphisms of C which fix Q_∞, they must also lie in T.

On the other hand, it is known that the Mordell-Weil group of C over $\mathbb{Q}(\mu_5)$ has rank zero [F] (see also [G-R]). Thus we could have deduced from this that the ten points in (3) must automatically lie in T. Finally we conclude that $C(\mathbb{Q}(\mu_5))$ consists of the three cusps and these ten points.

References

[C] R. Coleman: *p*-adic Abelian integrals and torsion points on curves, to appear.

[F] D.K. Faddeev: On divisor class groups of some algebraic curves, *Dokl. Tom. 136*: 296–298 (= Sov. Math., Vol. 2, No. 1: 67–69, 1961).

[G] R. Greenberg: On the Jacobian variety of some algebraic curves, Comp. 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.

[R] M. RAYNAUD: Courbes sur une variété abélienne 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.

(Oblatum 13-VII-1984 & 5-IX-1984)

Department of Mathematics
University of California
Berkeley, CA 94720
USA