Compositio Mathematica **106:** 1–9, 1997.

Torsion in Mordell-Weil groups of Fermat Jacobians

PAVLOS TZERMIAS
Department of Mathematics, University of California, Berkeley, CA 94720

Received 25 July 1995; accepted in final form 17 December 1995.

Abstract. We study the torsion in the Mordell-Weil group of the Jacobian of the Fermat curve of exponent p over the cyclotomic field obtained by adjoining a primitive p-th root of 1 to Q. We show that for all (except possibly one) proper subfields of this cyclotomic field, the torsion parts of the corresponding Mordell-Weil groups are elementary abelian p-groups.

Mathematics Subject Classifications (1991): 14H25, 14G05, 11D41.

Key words: Torsion, Mordell-Weil groups, Fermat Jacobians.

1. Introduction

Let Q be the field of rational numbers and let $\overline{Q}$ be a fixed algebraic closure of Q. Also let p be a fixed prime, where $p \geqslant 5$ and $p \neq 7$. The Fermat curve F_p is the projective nonsingular curve (over Q) given in projective coordinates by

$$F_p = \{(X, Y, Z) \in P^2(Q) \ : X^p + Y^p + Z^p = 0\}.$$

Let $K = Q(\zeta)$, where ζ is a fixed primitive p-th root of 1 in $\overline{Q}$. Let K^+ denote the maximal real subfield of K.

There are $3p$ points on F_p for which $XYZ = 0$, namely

$$a_j = (0, \epsilon\zeta^j, 1), \qquad b_j = (\epsilon\zeta^j, 0, 1), \qquad c_j = (\epsilon\zeta^j, 1, 0),$$

where ϵ is a primitive $2p$th root of 1 such that $\epsilon^2 = \zeta$ and $j = 0, 1, \ldots, p-1$. These points are all K-rational points and will be referred to as 'points at infinity' on F_p.

Also let J_p denote the Jacobian of F_p. The well-known Mordell–Weil theorem asserts that the group $J_p(K)$ of K-rational points on J_p is a finitely generated abelian group, hence it has a free part and a torsion part. There are some known bounds for the rank of the free part (see [3], [5], [10]). In addition, it follows easily from results in the literature that the torsion subgroup is a p-group (see Proposition 2.2 below). However, little is known about the precise structure of the torsion subgroup.

In this paper, we will prove some results on the torsion part $J_p(K)_{\text{torsion}}$ of $J_p(K)$. We prove that the group $pJ_p(K)_{\text{torsion}}$ is contained in a certain group G of order p^3, which we explicitly describe. This allows us to show that for all proper subfields L of K different than K^+, the group $pJ_p(L)_{\text{torsion}}$ is the zero group.

2. Background

In this section, we present some of the well-known facts about J_p.

We note the following automorphisms of F_p:

$$A\colon (X,Y,Z)\mapsto(\zeta X,Y,Z),$$

$$B\colon (X,Y,Z)\mapsto(X,\zeta Y,Z),$$

$$\rho\colon (X,Y,Z)\mapsto(Y,X,Z).$$

The automorphism B induces an endomorphism of the Jacobian J_p of F_p. We will denote this endomorphism by B as well, without fear of confusion. We also consider the elements $\pi = B-1$ and $\pi' = A-1$ of the endomorphism ring of J_p.

Now let s be an integer, where $1\leqslant s\leqslant p-2$. Consider the automorphism $g_s = AB^{-s}$ of F_p. We then consider the quotient of F_p by the action of the finite group generated by g_s. We obtain the curve $F_s = F_p/\langle g_s\rangle$ and call it a cyclic Fermat quotient.

Let $f_s\colon F_p\to F_s$ be the natural morphism.

The curve F_s has an affine equation $v^p = u^s(1-u)$ and the map f_s is given in affine coorinates by:

$$(x,y,1)\mapsto(u,v,1),$$

where $u = x^p$ and $v = x^s y$.

The curve F_s has an endomorphism $(u,v,1)\mapsto(u,\zeta v,1)$, which we shall also call B. It is clear that B commutes with f_s.

Let J_s denote the Jacobian of F_s. We have the endomorphism $\pi = B-1$ of J_s.

The map f_s induces a morphism (also denoted by f_s)

$$f_s\colon J_p\to J_s$$

and its dual

$$f_s^*\colon J_s\to J_p.$$

Now consider the maps

$$f=\prod_{s=1}^{p-2} f_s\colon J_p\to\prod_{s=1}^{p-2} J_s,$$

$$f^*=\sum_{s=1}^{p-2} f_s^*\colon \prod_{s=1}^{p-2} J_s\to J_p.$$

It can be proved (see [7]) that $f^*f = p$ on J_p. One simply proves that the two maps have the same effect on the differentials of the first kind on F_p. Therefore f is a Q-isogeny of J_p to a product of cyclic Fermat quotients.

https://doi.org/10.1023/A:1000189330893 Published online by Cambridge University Press

The following is an immediate consequence of what has been said above:

LEMMA 2.1. *For all s, the maps f_s, f_s^*, f, f^* all commute with π.*

Let l be a prime, such that $l \neq p$. Since K is unramified above l, it follows from Coleman's work (see Proposition 10 and Corollary 13.1 in [1]) that there are no l-torsion points on $J_s(K)$. This fact, combined with results of Greenberg (see [4]) and Kurihara (see [6]), shows that the group $J_s(K)_{\text{torsion}}$ equals the kernel of the isogeny π^3 of J_s.

Now, since f is a Q- isogeny of J_p onto the product of the J_s's and Ker(f) consists of points of order p, it immediately follows that:

PROPOSITION 2.2. *The group $J_p(K)_{\text{torsion}}$ is a p-group.*

3. Obtaining some information on $pJ_p(K)_{\text{torsion}}$

We can now prove the following:

THEOREM 3.1. *The group $J_p(K)_{\text{torsion}}$ is killed by $p\pi^2$.*

Proof. Let T be in $J_p(K)_{\text{torsion}}$. Then for $s = 1, 2, \ldots, p-2$, we have that $f_s(T) \;\epsilon\; J_s[\pi^3]$. Then Lemma 2.1 implies that $f_s(\pi^2 T) \;\epsilon\; J_s[\pi]$. But, by [5], $f_s^*(J_s[\pi]) = 0$. Therefore, for all s,

$$f_s^*(f_s(\pi^2 T)) = 0,$$

hence

$$p\pi^2 T = \sum_{s=1}^{p-2} f_s^*(f_s(\pi^2 T)) = 0,$$

which proves the theorem.

We are now able to obtain some information on $pJ_p(K)_{\text{torsion}}$. We will need an important result of Rohrlich (see Corollary 1 in [11]), which we restate here for the sake of convenience:

PROPOSITION 3.2 (Rohrlich). *A divisor of degree 0 supported at the points at infinity on F_p is principal if and only if, modulo p, it is in the span of*

$$\sum_{j=0}^{p-1} a_j, \qquad \sum_{j=0}^{p-1} b_j, \qquad \sum_{j=0}^{p-1} c_j,$$

$$\sum_{j=0}^{p-1} j(a_j + b_j), \qquad \sum_{j=0}^{p-1} j(b_j + c_j), \qquad \sum_{j=0}^{p-1} j(j+1)(a_j + b_j + c_j).$$

We now have:

LEMMA 3.3. *The Kernel of π on J_p equals the set of divisor classes of degree* 0 *that can be represented by a divisor supported only on the points b_j.*

Proof. Clearly any divisor class of degree 0 represented by a divisor supported only on the b_j's is in the kernel of π. Any such divisor class is of order p. The only principal such divisors are, modulo p, in the span of $b_0 + b_1 + \cdots + b_{p-1}$, by Proposition 3.2. Therefore, the cardinality of the set of these divisor classes of degree 0 equals p^{p-2}.

On the other hand, one can show (see [4]) that $\mathrm{Ker}(\pi^{p-1}) = \mathrm{Ker}(p)$, therefore $\mathrm{Ker}(\pi)$ has cardinality p^{p-2}, which proves the lemma.

Now, for a divisor D, let $[D]$ denote the class of D. Then we have the following:

PROPOSITION 3.4. *If a divisor class of degree* 0 *on J_p is invariant under both A and B, then it is a multiple of*

$$\left[\sum_{j=0}^{p-1} j(b_j - b_0)\right].$$

Proof. By Lemma 3.3, we can choose a representative D supported only on the points b_j, say

$$D = \sum_{j=1}^{p-1} x_j b_j - \left(\sum_{j=1}^{p-1} x_j\right) b_0.$$

Now since $\pi' D$ is principal, and since $Ab_j = b_{j+1}$, for $0 \leqslant j \leqslant p-2$ and $Ab_{p-1} = b_0$, we get that the divisor

$$\left(x_{p-1} + \left(\sum_{j=1}^{p-1} x_j\right)\right) b_0 - \left(x_1 + \left(\sum_{j=1}^{p-1} x_j\right)\right) b_1 + \sum_{j=2}^{p-1} (x_{j-1} - x_j) b_j$$

is also principal.

Since the only principal divisors supported on the b_j's are, modulo p, the multiples of $b_0 + b_1 + \cdots + b_{p-1}$, there exists an integer k such that, modulo p, we have

$$x_j = x_1 + (j-1)k,$$

for $j = 2, 3, \ldots, p-1$. Hence, modulo p, we have

$$D = \sum_{j=0}^{p-1} (x_1 + (j-1)k) b_j = \sum_{j=0}^{p-1} (x_1 - k + jk) b_j.$$

https://doi.org/10.1023/A:1000189330893 Published online by Cambridge University Press

But

$$\sum_{j=0}^{p-1}(x_1 - k)b_j$$

is principal, therefore the class of D is a multiple of

$$\left[\sum_{j=0}^{p-1} j(b_j - b_0)\right],$$

which proves the proposition.

We can now prove:

THEOREM 3.5.

$$p\pi J_p(K)_{\text{torsion}} \subseteq \left\langle \left[\sum_{j=0}^{p-1} j(b_j - b_0)\right] \right\rangle.$$

Proof. Let $T \epsilon J_p(K)_{\text{torsion}}$. Then, for all s, we have $\pi f_s(\pi T) \epsilon J_s[\pi]$. Therefore, as before, we get

$$0 = f_s^*(\pi f_s(\pi T)) = \pi \sum_{j=0}^{p-1}(AB^{-s})^j(\pi T).$$

Therefore the divisor class

$$D_s = \sum_{j=0}^{p-1}(AB^{-s})^j(\pi T)$$

is invariant under B. It is evidently also invariant under AB^{-s}, therefore it is invariant under both A and B.

Therefore, by Proposition 3.4, we get

$$D_s \epsilon \left\langle \left[\sum_{j=0}^{p-1} j(b_j - b_0)\right] \right\rangle.$$

This is true for all s, therefore we obtain that

$$p\pi T = \sum_{s=1}^{p-2} f_s^*(f_s(\pi T)) = \sum_{s=1}^{p-2} D_s$$

is also also a multiple of the divisor class of Proposition 3.4, which proves the theorem.

4. Bounding $pJ_p(K)_{\text{torsion}}$ effectively

Now we will prove the following:

PROPOSITION 4.1.

$$pJ_p(K)_{\text{torsion}} \subseteq \left\langle \left[\sum_{j=0}^{p-1} j(j+1)(a_j - a_0)\right], \quad \mathrm{Ker}(\pi) \right\rangle.$$

Proof. In view of Theorem 3.5, it suffices to show that

$$\pi \left[\sum_{j=0}^{p-1} j(j+1)(a_j - a_0)\right] \in \left\langle \left[\sum_{j=0}^{p-1} j(b_j - b_0)\right] \right\rangle.$$

We will use Proposition 3.2 again. We have the following equalities, *modulo p* :

$$\begin{aligned}
\pi \sum_{j=0}^{p-1} j(j+1)(a_j - a_0) &= \sum_{j=1}^{p-2} j(j+1)a_{j+1} - \sum_{j=1}^{p-2} j(j+1)a_j \\
&= \sum_{j=2}^{p-1} j(j-1)a_j - \sum_{j=1}^{p-2} j(j+1)a_j \\
&= (p-1)(p-2)a_{p-1} - 2a_1 - 2\sum_{j=2}^{p-2} ja_j \\
&= -2\sum_{j=0}^{p-1} ja_j \\
&= -2\sum_{j=0}^{p-1} j(a_j - a_0).
\end{aligned}$$

By Proposition 3.2, we have that the divisor

$$\sum_{j=0}^{p-1} j(a_j - a_0 + b_j - b_0)$$

is principal, which proves the proposition.

We now come to an effective bound on the cardinality of $pJ_p(K)_{\text{torsion}}$. Let

$$D_1 = \left[\sum_{j=0}^{p-1} j(j+1)(a_j - a_0)\right],$$

https://doi.org/10.1023/A:1000189330893 Published online by Cambridge University Press

$$D_2 = \left[\sum_{j=0}^{p-1} j(j+1)(b_j - b_0)\right],$$

$$D_3 = \left[\sum_{j=0}^{p-1} j(b_j - b_0)\right].$$

These divisor classes are linearly independent over Z/pZ, as one can easily show using Proposition 3.2.

Consider the group $G = \langle D_1,\ D_2,\ D_3\rangle$ generated by the above divisor classes. It has order p^3 and:

THEOREM 4.2. *We have:*

$$pJ_p(K)_{\text{torsion}} \subseteq G.$$

Proof. Recall the automorphism ρ of J_p, as defined in Section 2. Since $pJ_p(K)_{\text{torsion}}$ is invariant under ρ, we get, by Proposition 4.1, that

$$pJ_p(K)_{\text{torsion}} \subseteq \langle D_1,\ \text{Ker}(\pi)\rangle^{\rho} = \langle D_2,\ \text{Ker}(\pi')\rangle.$$

So if $D \,\epsilon\, J_p(K)_{\text{torsion}}$, then

$$pD = lD_2 + T,$$

where l is an integer and $\pi' T = 0$.

Multiply both sides of the above equality by π to get

$$p\pi D = \pi T.$$

By Theorem 3.5, we get that $\pi T \,\epsilon\, \langle D_3\rangle$, therefore

$$T \,\epsilon\, \langle D_1,\ \text{Ker}(\pi)\rangle.$$

But $\pi' T = 0$, so, by proposition 3.4, we get

$$T \,\epsilon\, \langle D_1,\ D_3\rangle,$$

therefore

$$pD \,\epsilon\, \langle D_1,\ D_2,\ D_3\rangle,$$

which proves the theorem.

5. Mordell–Weil groups over subfields of K

Now we will compute the action of $\text{Gal}(\overline{Q}/Q)$ on the divisor classes D_1, D_2, D_3 to obtain some results on the Mordell–Weil groups of J_p over subfields of K.

Let σ be an automorphism of $\overline{Q}$ over Q. Then $\sigma(\epsilon) = \epsilon^k$, for some integer k relatively prime to $2p$. Let $k = 2m + 1$, for some integer m. Then $\sigma(\zeta) = \zeta^k$.

Then $\sigma(a_j) = a_{kj+m}$ and $\sigma(b_j) = b_{kj+m}$, for all $j = 0, 1, \ldots, p-1$.

Then, modulo p, we have:

$$\begin{aligned} k^2\sigma\left(\sum_{j=0}^{p-1} j(j+1)(a_j - a_0)\right) &= \sum_{j=0}^{p-1} kj(kj+k)(a_{kj+m} - a_m) \\ &= \sum_{j=0}^{p-1} kj(kj+k)a_{kj+m} \\ &= \sum_{l=0}^{p-1}(l-m)(l+m+1)a_l \\ &= \sum_{l=0}^{p-1} l(l+1)a_l - m(m+1)\sum_{l=0}^{p-1} a_l. \end{aligned}$$

Therefore, again by Proposition 3.2, we get

$$k^2\sigma(D_1) = D_1.$$

Arguing in a similar way, we obtain:

$$k^2\sigma(D_2) = D_2,$$

$$k\sigma(D_3) = D_3.$$

These relations show immediately that D_3 is not defined over any proper subfield of K and also that D_1 and D_2 are both defined over K^+, but none of them is defined over any proper subfield L of K, where $L \neq K^+$. Therefore, we obtain the following theorems, as applications of Theorem 4.2:

THEOREM 5.1.

$$pJ_p(K^+)_{\text{torsion}} \subseteq \langle D_1,\ D_2\rangle.$$

THEOREM 5.2. *Let L be any proper subfield of K, $L \neq K^+$. Then*

$$pJ_p(L)_{\text{torsion}} = 0.$$

A final remark. It is known that (see [8], [12]) the automorphism group of F_p is the semidirect product of S_3 and $Z/pZ \times Z/pZ$. It turns out that the group G is invariant under the whole automorphism group G_p of F_p. It follows that if we

https://doi.org/10.1023/A:1000189330893 Published online by Cambridge University Press

consider the elements of the group ring $Z[G_p]$ as endomorphisms of J_p, then G is invariant under the action of $Z[G_p]$. A natural question that arises is whether there exists a K-endomorphism of J_p that does not preserve G. This would imply, in particular, that the bound on the cardinality of $pJ_p(K)_{\text{torsion}}$ (given by theorem 4.2) can be improved.

Lim (see [9]) has produced an example of a K-endomorphism of J_p that is not induced by $Z[G_p]$. To the author's disappointment, it turns out that this endomorphism annihilates G.

Acknowledgments

This paper is part of my doctoral dissertation at Berkeley. I am indebted to Robert Coleman for his constant support and guidance throughout the course of this work and to Hendrik Lenstra for motivating discussions. I also wish to thank David Rohrlich for his inspiring work on the Fermat curves, Ralph Greenberg for informing me of Kurihara's result (see [6]) and the referee for valuable suggestions regarding this paper.

References

1. Coleman, R. F.: *Torsion points on Abelian etale coverings of $P^1 - \{0,1,\infty\}$*, Transactions of the AMS, No. 1 (1989), 185–208.
2. Faddeev, D. K.: *On the divisor class groups of some algebraic curves*, Soviet Math. Dokl. 2 (1961), 67–69.
3. Faddeev, D. K.: *Invariants of divisor classes for the curves $x^k(1-x) = y^l$ in an l-adic cyclotomic field* (in Russian), Trudy Math. Inst. Steklov 64 (1961), 284–293.
4. Greenberg, R.: *On the Jacobian variety of some algebraic curves*, Compositio Math. 42 (1981), 345–359.
5. Gross, B. and Rohrlich, D.: *Some results on the Mordell-Weil group of the Jacobian of the Fermat curve*, Invent. Math. 44 (1978), 201–224.
6. Kurihara, M.: *Some remarks on conjectures about cyclotomic fields and K-groups of Z*, Compositio Math. 81 (1992), 223–236.
7. Lang, S.: *Introduction to algebraic and abelian functions*, GTM 89, Springer-Verlag, New York-Heidelberg-Berlin.
8. Leopoldt, H. W.: *Über die Automorphismengruppe des Fermatkörpers*, Journal of Number Theory (to appear).
9. Lim, C. H.: *Endomorphisms of Jacobian varieties of Fermat curves*, Compositio Math. 80 (1991), 85–110.
10. McCallum, W. G.: *The Arithmetic of Fermat curves*, Math. Ann. 294 (1992), 503–511.
11. Rohrlich, D.: *Points at infinity on the Fermat curves*, Invent. Math. 39 (1977), 95–127.
12. Tzermias, P.: *The group of automorphisms of the Fermat curve*, Journal of Number Theory 53 (1995), 173–178.