Journal de Théorie des Nombres
de Bordeaux **16** (2004), 577–585

The cuspidal torsion packet on hyperelliptic Fermat quotients

par David GRANT et Delphy SHAULIS

Résumé. Soit $\ell \geq 7$ un nombre premier, soit C la courbe projective lisse définie sur $\mathbb{Q}$ par le modèle affine $y(1-y)=x^\ell$, soit ∞ le point à l'infini de ce modèle de C, soit J la jacobienne de C et soit $\phi : C \to J$ le morphisme d'Abel-Jacobi associé à ∞. Soit $\overline{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$. Nous traitons ici un cas non couvert dans [12], en montrant que $\phi(C) \cap J_{\text{tors}}(\overline{\mathbb{Q}})$ est composé de l'image par ϕ des points de Weierstrass de C ainsi que les points $(x,y)=(0,0)$ et $(0,1)$ de C. Ici, J_{tors} désigne les points de torsion de J.

Abstract. Let $\ell \geq 7$ be a prime, C be the non-singular projective curve defined over $\mathbb{Q}$ by the affine model $y(1-y)=x^\ell$, ∞ the point of C at infinity on this model, J the Jacobian of C, and $\phi : C \to J$ the albanese embedding with ∞ as base point. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. Taking care of a case not covered in [12], we show that $\phi(C) \cap J_{\text{tors}}(\overline{\mathbb{Q}})$ consists only of the image under ϕ of the Weierstrass points of C and the points $(x,y)=(0,0)$ and $(0,1)$, where J_{tors} denotes the torsion points of J.

1. Introduction

En route to calculating the cuspidal torsion packets on Fermat curves, Coleman, Tamagawa, and Tzermias studied the cuspidal torsion packets on the quotients of Fermat curves [12]. Specifically, let ℓ be an odd prime, and for any $1 \leq a \leq \ell - 2$, let C_a be the non-singular projective curve defined over $\mathbb{Q}$ by the affine model $x^\ell = y(1-y)^a$, which is a curve of genus $g = (\ell-1)/2$. Let ∞ denote the lone point on C_a which is at infinity on this model, and $\phi : C_a \to J_a$ the Albanese embedding of C_a into its Jacobian J_a with ∞ as base point. By definition, the cuspidal torsion packet T_a is the set of torsion points of J_a which lie on $\phi(C_a)$. Let R_0 and R_1 respectively denote the points $(x,y)=(0,0)$ and $(0,1)$ on C. The following, and more general results, were proved in [12].

Manuscrit reçu le 14 février 2003.

Theorem (Coleman, Tamagawa, Tzermias)**.** *If $\ell \geq 11$, then there is an a, with $1 \leq a \leq \ell - 2$, such that C_a is not hyperelliptic, and such that*

$$T_a = \{\phi(\infty), \phi(R_0), \phi(R_1)\}.$$

This leaves open the question of determining T_a for any fixed a and ℓ, and in particular, for the a for which C_a is hyperelliptic, which we address here. It is known that C_a is hyperelliptic precisely when $a = 1, (\ell-1)/2$, or $\ell - 2$. There are isomorphisms from $C_{(\ell-1)/2}$ and $C_{\ell-2}$ to C_1, which induce bijections from $T_{(\ell-1)/2}$ and $T_{\ell-2}$ to T_1, so we will lose no generality in concentrating on C_1. Let $C = C_1$, $J = J_1$, and $T = T_1$. Note that on J the cuspidal torsion packet coincides with the hyperelliptic torsion packet. Let ζ denote a primitive ℓ^{th}-root of unity, let γ be a fixed ℓ^{th}-root of $1/4$, and let W_i, $1 \leq i \leq \ell$, denote the points $(\zeta^i\gamma, 1/2)$ on C.

Theorem 1.1. *Let $\ell \geq 7$. Then*

$$T = \{\phi(\infty), \phi(R_0), \phi(R_1)\} \cup \{\phi(W_i) | 1 \leq i \leq \ell\}.$$

Theorem 1.1 is due to Shaulis [20]. The exposition here incorporates some simplifications of the original argument. The case $\ell = 5$ does not exactly fit the pattern of Theorem 1.1, and in that case T is given explicitly in [9] and [5]. Indeed, Proposition 4.3(d) depends crucially on the assumption that $g \geq 3$.

The proof here owes heavily to the work of [12], but differs in some key respects. In particular, it does not rely on the p-adic integration theory of Coleman, which he used in [10] to show that T_a consists of just ℓ-power torsion if C_a is not hyperelliptic and $\ell \geq 11$, and that T consists of (2ℓ)-power torsion for $\ell \geq 5$. Our proof combines explicit geometry with the action of Galois groups on torsion points, an approach to Manin-Mumford problems that goes back to Lang [17], and has been used by many authors since. We refer the reader to the survey article of Tzermias for the history of the work on the Manin-Mumford Conjecture [23], and mention only some more recent work [2], [3], [4], [6], [7], [19], [22]. For results on the torsion of J_a that lies on a theta divisor, see [1], [13], and [21].

The next two sections of the paper are preliminary. In the first we detail what we need about the explicit geometry of C and J, and in the second we derive the necessary results on Galois actions on torsion points from the theory of complex multiplication. The proof of Theorem 1.1 is given in section 4.

We would like to thank the referee for a careful reading of this paper and a number of useful suggestions.

2. Geometry of C and J

We assume that $\ell \geq 7$. Let $K = \mathbb{Q}(\zeta)$, let $\overline{K}$ be an algebraic closure of K, and let $\mathcal{O} = \mathbb{Z}[\zeta]$ denote the ring of integers of K. Let $\lambda = 1 - \zeta$, so $\ell\mathcal{O} = (\lambda)^{\ell-1}$. Note that $\mathrm{Gal}(K/\mathbb{Q})$ consists of the automorphisms σ_i, $i \in (\mathbb{Z}/\ell\mathbb{Z})^*$, such that $\sigma_i(\zeta) = \zeta^i$.

The automorphism $\xi : (x, y) \to (\zeta x, y)$ of C extends to an automorphism Ξ of J, so we can endow J with complex multiplication by $\mathcal{O}$ by defining an embedding $\rho : \mathcal{O} \to \mathrm{End}(J)$ such that $\rho(\zeta) = \Xi$. Since $x^i dx/y$, $0 \le i \le g-1$ forms a basis for the holomorphic differentials of C, we get immediately (and it is well known) that the CM-type of J is $\Phi = \{\sigma_1, ..., \sigma_g\}$. We write $[\alpha]$ for $\rho(\alpha)$, and let $+$ denote the group morphism on J. For any $\alpha \in \mathcal{O}$ we let $J[\alpha]$ denote the kernel of $[\alpha]$ in $J(\overline{K})$ and $J[\alpha^\infty] = \cup_{n\ge 0} J[\alpha^n]$, and for any ideal $\mathfrak{a} \subseteq \mathcal{O}$, we let $J[\mathfrak{a}] = \cap_{\alpha\in\mathfrak{a}} J[\alpha]$. We identify points on J with the corresponding divisor class in $\mathrm{Pic}^0(C)$. Let O denote the origin on J.

The hyperelliptic involution $\iota : C \to C$ is given by $\iota((x, y)) = (x, 1-y)$, and its fixed points are the $2g+2$ Weierstrass points ∞ and W_i, $1 \le i \le \ell$.

The following results are standard.

Lemma 2.1. a) *For any P on C, $[-1]\phi(P) = \phi(\iota(P))$, so $[-1]^*$ preserves $\phi(C)$.*

b) *For any P on C, $[\zeta]\phi(P) = \phi(\xi(P))$, so $[\zeta]^*$ preserves $\phi(C)$.*

c) *Every point on J is represented by a unique divisor of the form*

$$P_1 + \cdots + P_r - r\infty \tag{1}$$

for some $0 \le r \le g$, and P_i on C, $1 \le i \le r$, where $P_i \ne \infty$, and $P_i \ne \iota(P_j)$ for $i \ne j$.

d) *The points in $J[2]$ are precisely those represented by a divisor of the form (1), where the P_i, $1 \le i \le r$, are distinct Weierstrass points.*

Lemma 2.1 immediately gives the following.

Lemma 2.2. *Let $Q \in J$ be represented by a divisor as in (1), and let $\phi(C)_Q$ denote the image of $\phi(C)$ under the translation-by-Q map. Then $\phi(C) \cap \phi(C)_Q$ is empty if $r \ge 3$, is $\{\phi(P_1), \phi(P_2)\}$ if $r = 2$, and is $\{\phi(P_1), O\}$ if $r = 1$.*

Indeed, if $\phi(P) = Q + \phi(P')$, then $P + \iota(P') - 2\infty$ and $P_1 + ... + P_r - r\infty$ represent the same point in J, which by Lemma 2.1 is impossible for $r \ge 3$, which implies that P is P_1 or P_2 for $r = 2$, and that P is P_1 or O for $r = 1$.

Recall that a point $Q \in J(\overline{K})$ is called *almost rational* over K, in the sense of Ribet [4], [19], if whenever $\tau(Q) + \upsilon(Q) = [2]Q$ for some $\tau, \upsilon \in \mathrm{Gal}(\overline{K}/K)$, then we have $\tau(Q) = \upsilon(Q) = Q$. We get the following from Lemma 2.1 and the fact that ∞ is K-rational.

Lemma 2.3. a) *The curve $\phi(C)$, and in particular the torsion packet T, are preserved under the action of $\mathrm{Gal}(\overline{K}/K)$.*

b) *Every $Q \in \phi(C) - J[2]$ is almost rational over K.*

We will need the following, which is Proposition C in [6].

Lemma 2.4. *Let k be a perfect field, G be a commutative algebraic group over k, and Ω be a finite set of primes. Let G_Ω denote the torsion points of G whose order is divisible only by primes in Ω, and Σ denote the subset of almost rational torsion points of G over k in G_Ω. For an odd prime p, set $\delta(p) = 1$, and set $\delta(2) = 2$. Define $A = \prod_{p\in\Omega} p^{\delta(p)}$. Let $k_1 = k(G[A])$, and suppose that there exist an integer B, divisible only by primes in Ω, such that $G(k_1) \cap G_\Omega \subseteq G[B]$. Then $\Sigma \subseteq G[B]$.*

Since the orders of the poles of x and y at ∞ are respectively 2 and ℓ, we see that for P on C, $\phi(P) \in J[\ell]-O$ if and only if there is a function on C of the form $y+f(x)$, where f is a polynomial of degree at most g, whose divisor is $\ell(P-\infty)$. If this is the case, then the divisor of $1-y+f(x)$ is $\ell(\iota(P)-\infty)$, so comparing divisors and matching up coefficients of x^ℓ gives $(y+f(x))(1-y+f(x)) = (x-x(P))^\ell$.

Lemma 2.5. $\#(\phi(C)\cap(J[\ell]-O)) \le \ell+2$.

Proof. The only points P on C with $x(P)=0$ are R_0 and R_1, and considering the divisors of y and $1-y$ shows that $\phi(R_0), \phi(R_1) \in J[\ell]-O$. Furthermore, if $\phi((z,w)) \in J[\ell]-O$ with $z \neq 0$, we get that $\phi((\zeta^i z, w))$ are distinct points in $J[\ell]-O$ for $i \in \mathbb{Z}/\ell\mathbb{Z}$. So it suffices to show that there are not two points (z,w) and (r,s) on C, with $zr \neq 0$ and $z^\ell \neq r^\ell$, such that $\phi((z,w)), \phi((r,s)) \in J[\ell]-O$.

If such (z,w) and (r,s) exist, then there are polynomials f and h of degree at most g such that

$$(y+f(x))(1-y+f(x)) = (x-z)^\ell, (y+h(x))(1-y+h(x)) = (x-r)^\ell.$$

Simplifying these gives

$$x^\ell + f(x) + f(x)^2 = (x-z)^\ell, x^\ell + h(x) + h(x)^2 = (x-r)^\ell. \tag{2}$$

Substituting $x = zX$ and dividing by z^ℓ in the former equation of (2), and substituting $x = rX$ and dividing by r^ℓ in the latter equation of (2), gives two expressions for $(X-1)^\ell$. Equating these yields

$$r^\ell f(zX)(f(zX)+1) = z^\ell h(rX)(h(rX)+1). \tag{3}$$

Letting u and v be square roots of z^ℓ and r^ℓ, (3) can be rewritten as

$$z^\ell - r^\ell = (u(2h(rX)+1)+v(2f(zX)+1))(u(2h(rX)+1)-v(2f(zX)+1)). \tag{4}$$

By assumption $z^\ell - r^\ell \neq 0$, so we get from (4) that $u(2h(rX)+1) \pm v(2f(zX)+1)$ are both constant polynomials, hence that $f(x)$ and $h(x)$ are both constants. But by (2) this violates the assumption that $zr \neq 0$. □

3. Galois actions on torsion points

Let H be the Hilbert class field of K. Recall that by using cyclotomic units, one can see that every principal ideal of $\mathcal{O}$ prime to (λ) has a generator congruent to 1 mod λ^2. Therefore, by Artin reciprocity, H is also the ray class field of K of conductor $(\lambda)^2$ (so also the ray class field of K of conductor (λ)).

Let $E = K(\gamma)$ and $L = E(\sqrt{\lambda})$. Recall that C has good reduction at every rational prime $p \neq \ell$, and it is shown in [11] that C, and hence J, achieves everywhere good reduction over L. For any extension of number fields F_1/F_2, let $D(F_1/F_2)$ denote the discriminant of F_1/F_2, and $N_{F_2}^{F_1}$ denote the norm from F_1 to F_2. If F_1/F_2 is a Galois extension, let G_{F_1/F_2} denote the Galois group of F_1/F_2. Finally, if F_1/F_2 is an abelian extension, let $\mathfrak{f}(F_1/F_2)$ denote the conductor of F_1/F_2.

Lemma 3.1. *We have* $\operatorname{ord}_{(\lambda)}(\mathfrak{f}(E/K)) \leq 2$.

Proof. This is a well-known argument that we briefly recall. The analogue to elliptic curves with complex multiplication plays a key role in the proof of the Coates-Wiles theorem (see [8], [15]).

If E/K is unramified over (λ) there is nothing to prove, so suppose it is ramified. Then it is totally ramified over (λ), so $\mathbb{Q}(\gamma)/\mathbb{Q}$ is totally ramified over ℓ. Hence $\operatorname{ord}_\ell(D(\mathbb{Q}(\gamma)/\mathbb{Q})) \geq \ell$. But for any $r \in \mathbb{Q}$, the polynomial discriminant of $x^\ell - r$ is $\pm r^{\ell-1}\ell^\ell$, so $\operatorname{ord}_\ell(D(\mathbb{Q}(\gamma)/Q)) = \ell$. Calculating the discriminant of $E/\mathbb{Q}$ two ways shows that $N_{\mathbb{Q}}^{K}(D(E/K))D(K/\mathbb{Q})^\ell = N_{\mathbb{Q}}^{\mathbb{Q}(\gamma)}(D(E/\mathbb{Q}(\gamma)))D(\mathbb{Q}(\gamma)/\mathbb{Q})^{\ell-1}$. The order at ℓ of the right-hand side is $(\ell-2) + \ell(\ell-1)$, so the order at ℓ of $N_{\mathbb{Q}}^{K}(D(E/K))$ is $2(\ell-1)$. Hence $\operatorname{ord}_{(\lambda)}(D(E/K)) = 2(\ell-1)$. Since all non-trivial characters on $G_{E/K}$ have the same conductor, the conductor-discriminant formula applied to E/K now gives the result. □

Lemma 3.2. *For any m and n coprime in $\mathbb{Z}$, $H(J[m^\infty])$ and $H(J[n^\infty])$ are linearly disjoint over H.*

Proof. Let $M = H(J[m^\infty]) \cap H(J[n^\infty])$. By the theory of complex multiplication, M is abelian over K, and by the criterion of Néron-Ogg-Shafarevich, since m and n are coprime, M/K is ramified only over (λ), so M/H is totally ramified at every prime over (λ). For the same reason, ML/L is unramified, so the ramification index over K of any prime of ML above (λ) divides $[L : K] = 2\ell$. Hence $[M : H]$ divides 2ℓ. Our goal is to show $[M : H] = 1$.

Suppose for a contradiction that $2|[M : H]$, so M/H has a quadratic subextension M'/H. Then since M' is totally ramified at every prime of H above (λ), $D(M'/H) = (\lambda)$. Since H/K is unramified, if h is the class number of K, $D(M'/K) = (\lambda)^h$. So the conductor-discriminant formula applied to M'/K gives that

$$(\lambda^h) = \prod_{\chi \in \hat{G}_{M'/K}} \mathfrak{f}_\chi \tag{5}$$

where $\mathfrak{f}_\chi$ is the conductor of the fixed field of χ over K. Note that $\mathfrak{f}_\chi$ is trivial if and only if the fixed field of χ is contained in H, which happens if and only if χ factors through $G_{M'/K}/G_{M'/H} \cong G_{H/K}$. Therefore $\mathfrak{f}_\chi$ is non-trivial for precisely $h = [H : K]$ choices of χ, and by (5), for each of these, $\mathfrak{f}_\chi = (\lambda)$. Hence the conductor of M'/K is also (λ). Since the ray class field of K of conductor (λ) is H, no such M' exists, and $[M : H]$ divides ℓ.

Finally suppose for a contradiction that $[M : H] = \ell$. Then since ML/L is unramified, the same must be true of ME/E. Therefore $ME = EI$, where I is the inertia subfield in ME of any prime of ME above (λ). Since (λ) does not divide $\mathfrak{f}(I/K)$, the formula for conductors of composite extensions and Lemma 3.1 imply that $\mathrm{ord}_{(\lambda)}(\mathfrak{f}(ME/K)) \leq 2$. Hence M is contained in the ray class field of K of conductor $(\lambda)^2$, which is H. □

If p is a rational prime, for every x in the p-adic integers $\mathbb{Z}_p$ and $u \in J[p^n]$, we define $[x]u = [x_n]u$, where $x_n \in \mathbb{Z}$ is such that $x \equiv x_n \mod p^n$.

Lemma 3.3. *Let $p \neq \ell$ be a rational prime. Then for every $x \in \mathbb{Z}_p^*$, there is a $\tau_x \in \mathrm{Gal}(\overline{K}/H)$ such that $\tau_x(u) = [x]u$ for every $u \in J[p^\infty]$.*

Proof. Since J has good reduction at p, it follows from Theorem 2.8 of Chapter 4 of [18] that $\mathrm{Gal}(H(J[p^\infty])/H)$ is isomorphic to $N_{\Phi'}((\mathcal{O}_p)^*)$, where $\mathcal{O}_p$ is the inverse limit as n goes to infinity of $\mathcal{O}/p^n$, and $N_{\Phi'}$ denotes the reflex norm (that is, for any $\alpha \in K$, $N_{\Phi'}(\alpha) = \prod_{\sigma\in\Phi} \sigma^{-1}(\alpha)$.) If $\epsilon = \zeta + \zeta^{-1}$, then $\mathbb{Z}[\epsilon]$ is the ring of integers of $K_0 = K(\epsilon)$, and since Φ is a set of representatives for the orbits of $G_{K/\mathbb{Q}}$ under the action of complex conjugation, the reflex norm restricted to K_0 is just the norm $N_{\mathbb{Q}}^{K_0}$. Then $N_{\mathbb{Q}}^{K_0}$ induces a norm map $N : \mathbb{Z}[\epsilon]_p^* \to \mathbb{Z}_p^*$, so it suffices to show that there is a $y \in \mathbb{Z}[\epsilon]_p^*$ such that $x = N(y)$. But via the Chinese Remainder Theorem, if $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$ are the primes of K_0 above p, then we have an isomorphism $\psi : \mathbb{Z}[\epsilon]_p^* \to \oplus_{i=1}^r \mathbb{Z}[\epsilon]_{\mathfrak{p}_i}^*$, where $\mathbb{Z}[\epsilon]_{\mathfrak{p}_i}$ is the valuation ring in $(K_0)_{\mathfrak{p}_i}$, the completion of K_0 at $\mathfrak{p}_i$. Furthermore, $(K_0)_{\mathfrak{p}_1}/\mathbb{Q}_p$ is an unramified extension of complete local fields and x is a unit in $\mathbb{Z}_p$, so there is a $z \in \mathbb{Z}[\epsilon]_{\mathfrak{p}_1}^*$ whose norm from $(K_0)_{\mathfrak{p}_1}$ to $\mathbb{Q}_p$ is x. We can then take y such that $\psi(y) = (z, 1, \ldots, 1)$, and we will have $N(y) = x$. □

Lemma 3.4. *There is a $\tau \in \mathrm{Gal}(\overline{K}/K)$ such that $\tau(u) = [1 + \ell]u$ for all $u \in J[\ell^\infty]$.*

Indeed, it is stated in the proof of Proposition 2 in [12] that there is such a $\tau \in \mathrm{Gal}(\overline{K}/\mathbb{Q})$, but the construction there shows that τ fixes K. It is also stated in [12] only for $\ell \geq 11$, but the same proof holds for $\ell = 7$.

4. Proof of Theorem 1.1

Suppose $t \in T$. If $t = O$, then $t = \phi(\infty)$, so from now on we assume $t \neq O$. We can uniquely write

$$t = t_2 + t_\lambda + t',$$

where $t_2 \in J[2^\infty]$, $t_\lambda \in J[\lambda^\infty]$, and t' is of order prime to 2λ.

Theorem 1.1 will follow directly from Propositions 4.1, 4.2, and 4.3.

Proposition 4.1. *We have $t' = O$.*

Proof. Let t' have order r. By applying Lemmas 3.2 and 3.3 to every prime dividing r, there exist a $\tau \in \mathrm{Gal}(\overline{K}/H)$ such that $\tau(t') = [2]t'$. Furthermore, applying Lemma 3.2 with $m = 2\ell$ and $n = r$, we can further assume that τ fixes t_2 and t_λ. Hence $\tau^2(t) + t + t = \tau(t) + \tau(t) + \tau(t)$, and $t, \tau(t), \tau^2(t)$ are all in $\phi(C)$ by Lemma 2.3. By Lemma 2.1, either $\tau(t) \in J[2]$, or $t = \tau(t)$. In either case, $t' = O$. □

Proposition 4.2. *If $t_2 \neq O$, then $t_\lambda = O$, and $t = t_2 = \phi(W_i)$, for some $1 \leq i \leq \ell$.*

Proof. Since $t_2 \neq O$, we claim that there is a $\tau \in \mathrm{Gal}(\overline{K}/H)$ such that $\tau(t_2) = t_2 + v$, for some $v \in J[2] - O$. Indeed, let 2^n be the smallest power of 2 such that $[2^n]t_2 = O$, so $n \geq 1$. If $n \geq 2$, from Lemma 3.3 we can let τ be an element such that $\tau(t_2) = [1 + 2^{n-1}]t_2$. Suppose now that $n = 1$. Lemma 2.1 shows that $H(J[2]) = H(\gamma)$, which is a non-trivial extension of H since (2) is unramified in H. If β is any non-trivial element in $\mathrm{Gal}(H(\gamma)/H)$, then $\beta(t_2) = [\zeta^j]t_2$ for some $1 \leq j \leq \ell - 1$. Hence in this case we can take $\tau = \beta$.

From Lemma 3.2, we can further assume that τ fixes t_λ. Then $\tau(t) = t + v$, so $\tau(t) \in \phi(C) \cap \phi(C)_v$. Lemmas 2.1 and 2.2 now imply that $t = \phi(W_i)$ for some $1 \leq i \leq \ell$. □

Proposition 4.3. *If $t_2 = O$, then $t = t_\lambda$ and*

a) $J(K(J[\ell])) \cap J[\ell^\infty] \subseteq J[\ell]$.
b) $t \in J[\ell]$.
c) $t \in J[\lambda^3]$.
d) $t \in J[\lambda]$.
e) $t = \phi(R_0)$ *or* $t = \phi(R_1)$.

Proof. a) Suppose $y \in J(K(J[\ell])) \cap J[\ell^\infty]$. By Lemma 3.4, there is a $\tau \in \mathrm{Gal}(\overline{K}/K)$ such that $\tau(x) = [1 + \ell]x$ for every $x \in J[\ell^\infty]$. Hence τ fixes $K(J[\ell])$, so $\tau(y) = y$. Therefore $y \in J[\ell]$.

b) Lemma 2.3 shows that $t \in J[\ell^\infty]$ is almost rational over K. Taking $\Omega = \{\ell\}$, $G = J$, and $k = K$ in Lemma 2.4, then part (a) gives that $t \in J[\ell]$.

c) Making use of results of Greenberg [14] and Kurihara [16], Lemma 2 of [12] gives that if $t \in J[\ell] - J[\lambda^3]$, then $\#(\phi(C) \cap J[\ell]) \geq \ell^2$. The proof there is stated for $\ell \geq 11$ but works equally well for $\ell = 7$. This violates Lemma 2.5, so $t \in J[\lambda^3]$.

d) This is Proposition 4 of [12] for $\ell \geq 11$, and in the hyperelliptic case is easy to do directly for any $\ell \geq 7$. Indeed, if $t \in J[\lambda^3]$, then $[(1+\zeta)(1-\zeta)^3]t = O$. Multiplying this out gives $t + [\zeta^3]t + [\zeta^3]t = [\zeta]t + [\zeta]t + [\zeta^4]t$, so by Lemma 2.1, either $[\zeta^3]t \in J[2]$, $t = [-\zeta^3]t$, $t = [\zeta]t$, or $t = [\zeta^4]t$. The first two possibilities give a contradiction, and the other possibilities imply that $t \in J[\lambda]$.

e) Note that $J[\lambda] = O \cup \cup_{i=1}^{g} \{[i]\phi(R_0), [i]\phi(R_1)\}$. The result now follows from Lemma 2.1.

□

References

[1] G. Anderson, *Torsion points on Jacobians of quotients of Fermat curves and p-adic soliton theory.* Invent. Math **118**, (1994), 475–492.

[2] M. Baker, *Torsion points on modular curves.* Invent. Math **140**, (2000), 487–509.

[3] M. Baker, B. Poonen, *Torsion packets on curves.* Compositio Math **127**, (2001), 109–116.

[4] M. Baker, K. Ribet, *Galois theory and torsion points on curves.* Journal de Théorie des nombres de Bordeaux **15**, (2003), 11–32.

[5] J. Boxall, D. Grant, *Examples of torsion points on genus 2 curves.* Trans. Amer. Math. Soc **352**, (2000), 4533–4555.

[6] J. Boxall, D. Grant, *Singular torsion on elliptic curves.* Mathematical Research Letters **10**, (2003), 847–866.

[7] F. Calegari, *Almost rational torsion points on semistable elliptic curves.* IMRN no. 10, (2001), 487–503.

[8] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer.* Invent. Math **39**, (1977), 223–251.

[9] R. F. Coleman, *Torsion points on Fermat curves.* Compositio Math **58**, (1986), 191–208.

[10] R. F. Coleman , *Torsion points on abelian étale coverings of* $\mathbb{P}^1 - \{0, 1, \infty\}$. Trans. AMS **311**, (1989), 185–208.

[11] R. F. Coleman, W. McCallum, *Stable reduction of Fermat curves and Jacobi sum Hecke characters J.* Reine Angew. Math **385**, (1988), 41–101.

[12] R. F. Coleman, A. Tamagawa, P. Tzermias, *The cuspidal torsion packet on the Fermat curve.* J. Reine Angew. Math **496**, (1998), 73–81.

[13] D. Grant, *Torsion on theta divisors of hyperelliptic Fermat jacobians.* Compositio Math. 140, (2004), 1432–1438.

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

[15] R. Gupta, *Ramification in the Coates-Wiles tower.* Invent. Math **81**, (1985), 59–69.

[16] M. Kurihara, *Some remarks on conjectures about cyclotomic fields and K-groups of* $\mathbb{Z}$. Composition Math **81**, (1992), 223–236.

[17] S. Lang, *Division points on curves.* Ann. Mat. Pura. Appl **70**, (1965), 229-234.

[18] S. Lang, *Complex Multiplication.* Springer-Verlag, New York, 1983.

[19] K. Ribet, M. Kim, *Torsion points on modular curves and Galois theory.* Notes of a talk by K. Ribet in the Distinguished Lecture Series, Southwestern Center for Arithmetic Algebraic Geometry, (May 1999).

[20] D. Shaulis, *Torsion points on the Jacobian of a hyperelliptic rational image of a Fermat curve.* Thesis, University of Colorado at Boulder, 1998.

[21] B. Simon, *Torsion points on a theta divisor in the Jacobian of a Fermat quotient.* Thesis, University of Colorado at Boulder, 2003.

[22] A. Tamagawa, *Ramification of torsion points on curves with ordinary semistable Jacobian varieties.* Duke Math. J **106**, (2001), 281–319.

[23] P. Tzermias, *The Manin-Mumford conjecture: a brief survey.* Bull. London Math. Soc. **32**, (2000), 641–652.

David Grant
Department of Mathematics
University of Colorado at Boulder
Boulder, CO 80309-0395 USA
E-mail : `grant@boulder.colorado.edu`

Delphy Shaulis
Department of Mathematics
University of Colorado at Boulder
Boulder, CO 80309-0395 USA
E-mail : `shaulis@euclid.colorado.edu`