Torsion on theta divisors of hyperelliptic Fermat Jacobians

David Grant

Abstract

We generalize a result of Anderson by showing that torsion points of certain orders cannot lie on a theta divisor in the Jacobians of hyperelliptic images of Fermat curves. The proofs utilize the explicit geometry of hyperelliptic Jacobians and their formal groups at the origin.

Introduction

Let $\ell$ be an odd prime, $\zeta$ a primitive $\ell$th-root of unity, $K = \mathbb{Q}(\zeta)$, and $\lambda = 1 - \zeta$, a generator for the lone prime of the ring of integers $\mathbb{Z}[\zeta]$ of $K$ that lies over $\ell$. 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 $x^a = y(1-y)^a$. We let $\infty$ denote the lone point on $C_a$ which is at infinity on this model. Note that $C_a$ is an image of the $\ell$th Fermat curve, and has genus $g = (\ell - 1)/2$. Let $J_a$ denote the Jacobian of $C_a$, and $\phi : C_a \to J_a$ be the embedding sending a point $P \in C_a$ to the point of $J_a$ corresponding to the divisor class of $P - \infty$. For any $m \geq 1$ we extend $\phi$ to a map on the $m$th-symmetric product $C_a^{(m)}$ of $C_a$, and let $\Theta = \phi(C_a^{(g-1)})$.

The automorphism $(x, y) \to (\zeta x, y)$ of $C_a$ extends to an automorphism $\xi$ of $J_a$, so we can endow $J_a$ with complex multiplication (CM) by $\mathbb{Z}[\zeta]$ by defining an embedding $\iota : \mathbb{Z}[\zeta] \to \text{End}(J_a)$ such that $\iota(\zeta) = \xi$. We write $[\alpha]$ for $\iota(\alpha)$. Let $\overline{K}$ be an algebraic closure of $K$. For any $\alpha \in \mathbb{Z}[\zeta]$, we let $J_a[\alpha]$ denote the kernel of $[\alpha]$ in $J_a(\overline{K})$, and for any ideal $\mathfrak{a} \subseteq \mathbb{Z}[\zeta]$, we let $J_a[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} J_a[\alpha]$. The following was proved in [And94].

Theorem (Anderson). Let $\mathfrak{p}$ be a first degree prime of $\mathbb{Z}[\zeta]$. Then $J_a[\mathfrak{p}] \cap \Theta = J_a[\lambda] \cap \Theta$.

For any $a \subseteq \mathbb{Z}[\zeta]$, let $J_a(a)^*$ denote the non-trivial elements of $J_a[a]$, and for any point $Q \in J_a(\overline{K})$, let $T_Q$ denote the translation-by-$Q$ map on $J_a$. Let $Z$ be the point $(0, 0)$ on $C$ and $P = \phi(Z)$. Since $J_a[a]$ is generated by $P$, Anderson’s theorem is equivalent to the statement that $J_a[\mathfrak{p}]^* \cap T_{\mathfrak{p}}^* \Theta$ is empty for all $0 \leq v \leq \ell - 1$. The goal of this paper is to extend Anderson’s result as best as we can to powers of primes of $\mathbb{Z}[\zeta]$ of arbitrary degree, at least in the case that $C_a$ is hyperelliptic, when the geometry of $J_a$ is more tractable. We note that for $1 \leq a \leq \ell - 2$, the only $C_a$ which are hyperelliptic are $C_1$, $C_{(\ell-1)/2}$, and $C_{\ell-2}$. Since there are isomorphisms from $C_{(\ell-1)/2}$ to $C_1$ which induce isomorphisms from $\Theta$ on $J_{(\ell-1)/2}$ and $J_{\ell-2}$ to $\Theta$ on $J_1$ translated by a $\lambda$-torsion point, we will lose no generality by concentrating on $C_1$.

Let $C = C_1$ and $J = J_1$. For any $i \in (\mathbb{Z}/\ell\mathbb{Z})^*$, let $\sigma_i \in G = \text{Gal}(K/\mathbb{Q})$ be such that $\sigma_i(\zeta) = \zeta^i$. It is well known (and we will see in §2) that the CM-type of $J$ is $\Phi = \{\sigma_1, \ldots, \sigma_\ell\}$.

We prove two theorems.

Received 27 November 2002, accepted in final form 31 July 2003, published online 15 October 2004.

2000 Mathematics Subject Classification 11G10, 14K12.

Keywords: Fermat curves, torsion.

This journal is © Foundation Compositio Mathematica 2004.
THEOREM 1. Let \( p \) be a first or second degree prime of \( \mathbb{Z}[\zeta] \). Then for any \( n \geq 1 \), \( J[\lambda p^n] \cap \Theta = J[\lambda] \cap \Theta \).

The theorem is proved in § 2 by showing that certain functions \( h_v \) on \( J \), \( 1 \leq v \leq g \), which vanish on \( T_{(\mathbb{Z}_p - v)\mathbb{P}}^*(\Theta) \), have non-zero \( p \)-adic absolute value when evaluated at \( J[\mathbb{P}^n] \). Since \( J[\mathbb{P}^n] \) lies in the kernel of reduction of \( J \) mod \( p \), this is achieved by using the formal group \( F \) on the kernel of reduction mod \( p \) to compute the \( p \)-adic absolute values of certain parameters \( s_i \) at the origin of \( J \) evaluated at \( J[\mathbb{P}^n] \), \( 1 \leq i \leq g \), and then by expanding \( h_v \) in the local ring at the origin in terms of the \( s_i \).

The formal group calculation crucially depends on the assumption that \( p \) is a first or second degree prime. Indeed, if \( \pi \in \mathbb{Z}[\zeta] \) is a uniformizer at \( p \) and prime to all of its other conjugates, then the \( \mathbb{P}^n \)-torsion in \( F \) coincides with \( \mathbb{P}^n \)-torsion, and we compute the \( p \)-adic absolute value of \( s_i \) evaluated at \( \mathbb{P}^n \)-torsion by applying the formal implicit function theorem to \( [\mathbb{P}^n] \), thought of as an endomorphism of \( F \). This requires that the rank of the Jacobian of \( [\pi] \) mod \( p \) is \( g - 1 \), which only happens when the intersection of \( \Phi \) and the decomposition group \( G_0 \) of \( p \) in \( G \) is the identity.

The assumption that \( C \) is hyperelliptic is used only to explicitly produce the \( s_i \) and the \( h_v \), and in § 1 to compute the expansions of the \( h_v \) in terms of the \( s_i \). It may well be that a more clever geometric argument will produce analogous results in the case that \( C_a \) is not hyperelliptic. Indeed, since this paper was written, using Galois-theoretic techniques, Simon has shown that Theorem 1 holds for any \( J_a \) as long as \( p \) has norm greater than some explicit function of \( \ell \) and the CM-type of \( J_a \) is non-degenerate. Simon also has some remarkable results constraining the orders of torsion points on the theta divisor of \( J_a \) when the orders are not necessarily the power of a single prime \([Sim03]\).

There are, however, some cases when we can use formal groups to generalize Theorem 1 to primes of arbitrary degree. Let \( p \neq (\lambda) \) be any prime of \( \mathbb{Z}[\zeta] \), \( p \) the rational prime it lies over, and \( f = \#(G_0) \). Let \( s \) be the number of cosets of \( G_0 \) in \( G \) which have non-trivial intersection with \( \Phi \), let \( W_r \), \( 1 \leq r \leq s \), denote these intersections, and \( d_r = \#(W_r) \). We arbitrarily choose an element \( \sigma_{m_r} \in W_r \) for each \( 1 \leq r \leq s \). Given these choices we form a double indexed permutation \( \omega(r, j) \), \( 1 \leq r \leq s \), \( j \in \mathbb{Z}/d_r \mathbb{Z} \), of \( (1, \ldots, g) \), by picking \( \omega(r, j) \) such that \( \sigma_{\omega(r, j)} \in W_r \), and if \( \omega(r, j) \equiv m_r p^{e_{r,j}} \mod \ell \), with \( 0 \leq e_{r,j} < f \), then \( 0 = e_{r,1} < \cdots < e_{r,d_r} \).

For any integer \( i \), let \( (i) \) denote the least non-negative residue of \( i \) modulo \( f \). For each \( 1 \leq r \leq s \) and \( j \in \mathbb{Z}/d_r \mathbb{Z} \), we set \( E_{r,j} = \sum_{i \in \mathbb{Z}/d_r \mathbb{Z}} P_i^{(e_{r,j} - e_{r,i})} \). If \( r \) is such that there is a unique \( j' \in \mathbb{Z}/d_r \mathbb{Z} \) such that \( E_{r,j'} \) is minimal, we say that \( \omega(r, j') \) is admissible for \( p \). Let \( \lceil \cdot \rceil \) denote the greatest integer function. If \( 0 \leq q \leq g - 1 \) is such that \( \lceil (g + q + 1)/2 \rceil = \omega(r, j') \) for some \( \omega(r, j') \) admissible for \( p \), then we call \( q \) good for \( p \). Let \( A_p \) denote the set of all \( q \) which are good for \( p \), which depends only on the residue class of \( p \) mod \( \ell \).

THEOREM 2. \( J[\mathbb{P}] \cap T_{v \mathbb{P}} \Theta \) is empty for all \( v \in \pm(A_p \cup \{g\}) \).

Note that when \( p \) is a second or degree prime, then Theorem 2 reduces to Theorem 1 in the case \( n = 1 \). The first improvement comes when \( \ell = 5 \), but in this case \( J[\mathbb{P}] \cap \Theta \) has been explicitly determined (see [BG00] or [Col86]). When \( \ell = 7 \), we get that \( J[\mathbb{P}] \cap T_{v \mathbb{P}}^* \Theta \) is empty for: all \( v \) when \( p \equiv 2 \) mod \( 7 \); \( v = 0, \pm 1, \pm 3 \) when \( p \equiv 3 \) mod \( 7 \); \( v = \pm 2, \pm 3 \) when \( p \equiv 4 \) mod \( 7 \); and \( v = \pm 3 \) when \( p \equiv 5 \) mod \( 7 \).

The reason for the rather arcane hypotheses for Theorem 2 is that the \( p \)-adic absolute values of the \( s_i \) evaluated at \( [\pi] \)-torsion can no longer be calculated via the implicit function theorem, and are instead calculated (in [Gra]) for parameters \( S_i \) of a \( p \)-typical formal group isomorphic to \( F \) (see [Haz78]). The hypotheses are necessary to ensure that we can glean information on the \( p \)-adic absolute values of the \( s_i \) evaluated at \( [\pi] \)-torsion from the absolute values of the \( S_i \).
To the author’s taste, the proofs given here have some of the same flavor as Anderson’s proof, without sharing many of the ingredients.

1. Expansions of functions on $J$

Let $k$ be any field of characteristic other than $\ell$, so that $C$ defines a hyperelliptic curve of genus $g = (\ell - 1)/2$ over $k$, with hyperelliptic involution $\gamma(x, y) = (x, y)$, where $y = 1 - x$. We will identify points of $J$ with the corresponding divisor classes in $\text{Pic}^0(C)$. We write $D_1 \sim D_2$ to denote that two divisors on a variety are linearly equivalent, and let $\text{cl}(D)$ be the class of a divisor $D$ modulo linear equivalence. It is well known that for any $Q \in C$, $Q + \gamma(Q) \sim 2\infty$, and that every divisor class $D \in \text{Pic}^0(C)$ can be uniquely represented by a divisor of the form $P_1 + \cdots + P_r - r\infty$ for some $r \leq g$, where $P_i \neq \infty$, and for $i \neq j$, $P_i \neq \gamma(P_j)$. In particular, $[-1](P_1 + \cdots + P_r - r\infty) = \gamma(P_1) + \cdots + \gamma(P_r) - r\infty$. Hence, $\Theta$ consists of divisor classes of the form $\text{cl}(P_1 + \cdots + P_g - g\infty)$, where $P_i \neq \infty$ and $P_i \neq \gamma(P_j)$ for $i \neq j$.

Via the surjective birational map $\phi : C(g) \to J$, we identify symmetric functions on $C^g$ with functions on $J$. Since $Z = (0, 0) \in C$ is not fixed by $\gamma$, $gZ$ is not a special divisor on $C$, and if $P = \phi(Z)$, $gP \notin \Theta$. So if $E \in C(g)$ is the image of the $g$-tuple $(Z, \ldots, Z)$ under the natural projection from $C^g$ to $C(g)$, then $\phi$ is an isomorphism in a neighborhood of $E$, and induces an isomorphism between completed local rings $\hat{O}_{J,gP}$ and $\hat{O}_{C(g),E}$. As in [Mil86], the latter is generated as a power series ring over $k$ by the elementary symmetric functions $e_1, \ldots, e_g$ in any local parameter $\tau$ of $C$ at $Z$. We always take $\tau = x$, and if $P_i = (x_i, y_i)$, $1 \leq i \leq g$, are independent generic points of $C$, we set $t_i = e_i(x_1, \ldots, x_g)$, so that $t_1, \ldots, t_g$ form a set of local parameters of $J$ at $gP$. Our goal in this section is to write down functions $B_v$ on $J$, $1 \leq v \leq g$ (determined up to constant multiples), with divisors $vT_1^*\Theta + T_{-vP}^*\Theta - (v+1)\Theta$, and to calculate the lead term of the expansion of $B_v$ in $\hat{O}_{J,gP}$ in terms of $t_1, \ldots, t_g$. We employ the techniques and some of the results of [AG01].

Let $H \subset J$ be the irreducible divisor on $J$ representing divisor classes in $\text{Pic}^0(C)$ of the form $\{\text{cl}(2Q_1 + Q_2 + \cdots + Q_g - g\infty) \mid Q_i \in C\}$. If $g = 1$, we take $H$ to be the zero divisor.

For any functions $F_i \in k(C)$, and points of $C$, $1 \leq i \leq g$, let

$$D(F_1, \ldots, F_g)(Q_1, \ldots, Q_g)$$

denote the determinant $\det(F_i(Q_j))_{1 \leq i, j \leq g}$.

As before, let $P_i = (x_i, y_i)$, $1 \leq i \leq g$, denote independent generic points on $C$, so $U = P_1 + \cdots + P_g - g\infty$ is a generic point on $J$. For any $1 \leq v \leq g$, let

$$M_v = D(x^v, \ldots, x^a, y, \ldots, y^b)(P_1, \ldots, P_g),$$

$$N_v = D(x^v, \ldots, x^a, y, \ldots, y^b)(\gamma(P_1), \ldots, \gamma(P_g))$$

$$= D(x^v, \ldots, x^a, y, \ldots, y^b)(P_1, \ldots, P_g),$$

where $a = [g + (v - 1)/2]$, $b = [(v - 2)/2]$. If $b = -1$, then $v = 1$, and by convention the function $y$ is omitted from the definitions of $M_1$ and $N_1$.

**Proposition 1.** For any $1 \leq v \leq g$, we can take $B_v = N_v/\prod_{1 \leq i < j \leq g}(x_i - x_j)$.

In the case $v = 1$, we have $N_1/\prod_{1 \leq i < j \leq g}(x_i - x_j) = \pm t_g$, in which case the result follows from [AG01, Proposition 5]. So we assume now that $b \geq 0$. We need a few lemmas. We first investigate where $M_v$ and $N_v$ vanish when we specialize $P_1, \ldots, P_g$.

**Lemma 1.** If $U \in J - \Theta - H - T_{-P}^*\Theta - T_{-P}^*\Theta$, then $M_v(P_1, \ldots, P_g) = 0$ if and only if $U \in T_{-P}^*\Theta$, and $N_v(P_1, \ldots, P_g) = 0$ if and only if $U \in T_{-P}^*\Theta$.  

1434
Proof. If \( U \in T_{vP}^\ast\Theta \), then \( U + vP \in \Theta \), so there exist \( Q_1, \ldots, Q_{g-1} \in C \) such that \( P_1 + \cdots + P_g + Q_1 + \cdots + Q_{g-1} \sim (2g + v - 1)\infty - vZ \), hence a function \( f \in \mathcal{L}((2g + v - 1)\infty - vZ) \) which vanishes at \( P_1, \ldots, P_g \). Since \( x^a, x^a, y, \ldots, yx^b \) form a basis for \( \mathcal{L}((2g + v - 1)\infty - vZ) \), there is a non-trivial linear combination of \( x^a, x^a, y, \ldots, yx^b \) which vanishes at \( P_1, \ldots, P_g \), so \( M_v(P_1, \ldots, P_g) = 0 \). The converse and the corresponding results for \( N_v(P_1, \ldots, P_g) \) are similar. \( \square \)

Since the function \( M_vN_v \) is symmetric in \( P_1, \ldots, P_g \), we can consider it as a function \( F(U) \) on \( J \). Since it is regular on \( C^{(g)} \) except where some \( P_i \) is specialized to \( \infty \), on \( J \) it is regular on \( J - \Theta \). The precise order of its pole at \( \Theta \) can be read off by the recipe of [AG01, Lemma 1, and is computed to be \( 4g + 2v - 2 \). Since \( \Theta, H, \) and \( F \) are invariant under \([-1]^\ast \), we get that the divisor \( (F) \) of \( F \) is of the form

\[
(F) = m(T_v^\ast\Theta + T_{-vP}^\ast\Theta) + j(T_v^\ast\Theta + T_{-P}^\ast\Theta) + nH - (4g + 2v - 2)\Theta,
\]

for some \( m \geq 1, j \geq 0, \) and \( n \geq 0 \). It is clear that \( M_vN_v \) vanishes on \( H \), so \( n \geq 1 \), and if the characteristic of \( k \) is 2, then each of \( M_v \) and \( N_v \) are functions on \( J \) that vanish at \( H \), so \( n \geq 2 \).

Lemma 2. We have \( j \geq v \).

Proof. Again, it follows from [AG01, Proposition 5] that the divisor of \( t_g = x_1 \cdots x_g \) is \( T_v^\ast\Theta + T_{-P}^\ast\Theta - 2\Theta \), so is a uniformizer for \( T_v^\ast\Theta \) and \( T_{-P}^\ast\Theta \). Expanding \( M_vN_v \) in \( \hat{O}_{I,gP} \) using \( y_i = x_i^1 + \cdots, 1 \leq i \leq g \), in \( \hat{O}_{C,Z} \), we get that \( F/t_v^u \) is a power series in \( t_1, \ldots, t_g \), and hence is regular at \( gP \), which gives the lemma. \( \square \)

Let \( \Delta(U) = \prod_{1 \leq i < j \leq g} (x_i - x_j)^2 \). It is shown in [AG01, Proposition 7] that the divisor of \( \Delta \) is \( n'H - (4g - 1)\Theta \), where \( n' = 2 \) if the characteristic of \( k \) is 2 and \( n' = 1 \) otherwise.

Lemma 3. We have \( (F/\Delta) = T_v^\ast\Theta + T_{-vP}^\ast\Theta + v(T_v^\ast\Theta + T_{-P}^\ast\Theta) - (2v + 2)\Theta \).

Proof. It follows from (1) and Lemma 2 that

\[
(F/\Delta) = m(T_v^\ast\Theta + T_{-vP}^\ast\Theta) + j(T_v^\ast\Theta + T_{-P}^\ast\Theta) + I - (2v + 2)\Theta,
\]

for some \( m \geq 1 \) and \( j \geq v \), where \( I \) is some effective divisor. However, by the theorem of the square, \( T_v^\ast\Theta + T_{-vP}^\ast\Theta \sim T_v^\ast\Theta + T_{-P}^\ast\Theta \sim 2\Theta \), so \( I = 0, j = v \), and \( m = 1 \). \( \square \)

Proof of Proposition 1. Lemma 3 states that

\[
F_M(U) = M_v/ \prod_{1 \leq i < j \leq g} (x_i - x_j), \quad F_N(U) = N_v/ \prod_{1 \leq i < j \leq g} (x_i - x_j),
\]

are functions on \( J \), such that the sum of the divisors \( (F_M) + (F_N) \) is

\[
T_v^\ast\Theta + T_{-vP}^\ast\Theta + v(T_v^\ast\Theta + T_{-P}^\ast\Theta) - (2v + 1)\Theta.
\]

Note that \( F_N = [-1]^\ast F_M \). We get immediately that the polar divisors of \( F_M \) and \( F_N \) are each \((v + 1)\Theta \), and by Lemma 1, using the irreducibility of \( \Theta \) and the theorem of the square, that

\[
(F_N) = vT_v^\ast + T_{-vP}^\ast - (v + 1)\Theta,
\]

so we can take \( B_v = F_N \). \( \square \)

Proposition 2. Take \( 1 \leq v \leq g \). Let \( c = a - v + 1 = [g + (1 - v)/2] \) and \( d = v - b - 1 = [(v + 1)/2] \). The lead term in the expansion of \( B_v \) in \( \hat{O}_{I,gP} \) in terms of \( t_1, \ldots, t_g \) is

\[
\pm \det(t_c-i+j)_{1 \leq i,j \leq d},
\]

so is of degree \( d \), and includes the monomial \( \pm t_c^d \).
Proof. Note that the statement of the theorem makes sense, since for \(1 \leq i, j \leq d\), we have \(1 \leq c - i + j \leq g\). Note also that the case \(v = 1\) follows from the choice \(B_1 = \pm t_g\), so we can assume \(b > 0\).

Recall that if \(\nu = (\nu_1, \ldots, \nu_g)\) is a \(g\)-tuple of exponents, then the generalized Vandermonde determinant \(a_\nu\) in variables \(z_1, \ldots, z_g\) is \(\det(z_{i,j}^{\nu_j})_{1 \leq i, j \leq g}\), and permuting the entries of \(\nu\) changes \(a_\nu\) by at most a sign. In particular, if \(\delta\) is the \(g\)-tuple \((g - 1, g - 2, \ldots, 1, 0)\), then \(a_\delta\) is the standard Vandermonde determinant. An \(L\)-tuple of positive integers \(\eta = (\eta_1, \ldots, \eta_L)\), \(\eta_1 \geq \cdots \geq \eta_L\), is called a partition of length \(L\). If \(L \leq g\), we can append zeros to \(\eta\) to make it a \(g\)-tuple, and define \(s_\eta = a_{\eta+\delta}/a_\delta\), which is called the Schur function corresponding to \(\eta\) (see [Mac79]). Recall that the conjugate partition of \(\eta\) is defined to be the partition \(\mu = (\mu_1, \ldots, \mu_m)\), where \(m = \eta_1\), and \(\mu_i = \#\{1 \leq j \leq L|\eta_j \geq i\}\). It is shown in [Mac79, p. 41], that

\[
s_\eta = \det(e_{\mu_i-i+j})_{1 \leq i, j \leq m}, \tag{3}
\]

where \(e_\epsilon\) denotes the \(\epsilon\)-th-elementary symmetric function in \(z_1, \ldots, z_g\), with the convention that \(e_0 = 1\), and \(e_\epsilon = 0\) for \(\epsilon < 0\) or \(\epsilon > g\).

Using that \(y = \sum_{i \geq 1} \kappa_i e_i^d\) in \(\hat{O}_{C, Z}\), with \(\kappa_i = (2(i-1))!/i!(i-1)!\), we get that \(N_v\) can be expanded as an infinite sum of generalized Vandermonde determinants in \(x_1, \ldots, x_g\), with exponent vectors

\[
(v, v+1, \ldots, a_i, i_0 \ell, i_1 \ell + 1, \ldots, i_b \ell + b), \tag{4}
\]

\(i_j \geq 0, 0 \leq j \leq b\), and coefficients \(\pm \prod_{j=0}^{b} \kappa_{i,j}\) (where we set \(\kappa_0 = 1\)). Hence, \(B_v\) can be expanded as an infinite sum of Schur functions \(s_\eta\) in \(x_1, \ldots, x_g\), with coefficients \(\pm \prod_{j=0}^{b} \kappa_{i,j}\), where \(\eta\) depends on the choice of \(i_0, \ldots, i_b\). Let us first calculate \(s_\eta\) when \(i_0 = \cdots = i_b = 0\). Ordering (4) from largest to smallest gives \((a, v, b, \ldots, 0)\) for \(\eta + \delta\), so \(\eta\) is the partition \((d, \ldots, d)\) of length \(c\). Hence, the conjugate \(\mu\) of \(\eta\) is the partition \((c, \ldots, c)\) of length \(d\). So by (3), \(\pm s_\eta\) is the determinant in the statement of the proposition. It remains to be shown that the total degree of every monomial in \(s_\eta\) for the \(\eta\) corresponding to any other choice of \(i_0, \ldots, i_b\) is greater than \(d\).

Suppose now that for some \(0 < r \leq b + 1\), \(r\) of the \(i_j\) are positive, and we have reordered (4) from largest to smallest, so for some permutation \(j_1, \ldots, j_{b+1}\) of \(0, \ldots, b\), we get that \(\eta + \delta\) is

\[
(i_{j_1} \ell + 1, \ldots, i_{j_r} \ell + j_r, a, \ldots, v, j_{b+1}, \ldots, j_{b+1}).
\]

Subtracting \(\delta\) to find \(\eta\) shows that \(\eta_i \geq d + r\) for all \(1 \leq i \leq c + r\). Hence, the conjugate partition \(\mu\) to \(\eta\) has \(\mu_i \geq c + r\) for all \(1 \leq i \leq d + r\). In particular, if \(m = \eta_1\), since \(c \geq d\), \(e_0\) does not appear in the first \(d + r\) columns of the matrix \([e_{\mu_i-i-j}]_{1 \leq i, j \leq m}\). Hence, by (3), every monomial in \(s_\eta\) has total degree at least \(d + r > d\), so we are done.

2. Proofs of the theorems

From the results of § 1, we see that \(s_i = T_g \rho L_{g i}, 1 \leq i \leq g\), form a system of parameters for \(J\) at the origin \(O\), for \(J\) defined over \(K\), or for \(J\) defined over any residue field \(\mathbb{Z}[\zeta]/p\), for any prime \(p \subseteq \mathbb{Z}[\zeta]\) other than \((\lambda)\). As a result, \(s_i, 1 \leq i \leq g\), are a set of parameters for the formal group \(\mathcal{F}\) of \(J\) at the origin defined over \(\mathbb{Z}[1/\ell][\zeta]\). Furthermore, for any \(\alpha \in \mathbb{Z}[\zeta]\), we have power series \(\rho(\alpha)_i, 1 \leq i \leq g\), with coefficients in \(\mathbb{Z}[1/\ell][\zeta]\), such that \([\alpha]^* s_i = \rho(\alpha)_i(s_1, \ldots, s_g)\) in \(\mathcal{O}_{J, o}\). The map \(\alpha \to \rho(\alpha) = (\rho(\alpha)_1, \ldots, \rho(\alpha)_g)\) gives an embedding of \(\mathbb{Z}[\zeta]\) into the endomorphism ring of \(\mathcal{F}\). Since \(g P\) is fixed by \([\zeta]\), we see that \([\zeta]^* s_i = \zeta^* s_i\), confirming that \(\Phi\) is the CM-type of \(J\). Therefore,

\[
\rho(\alpha)_i(s_1, \ldots, s_g) = \sigma_1(\alpha)s_i + (d^\alpha \geq 2), \tag{5}
\]

where \((d^\alpha \geq n)\) denotes a power series, all of whose terms have total degree at least \(n\).
Let $p \neq (\lambda)$ be a prime of $K$, and for all $i \in \mathbb{Z}/\ell \mathbb{Z}^*$, let $p_i = \sigma_i(p)$, and let $K_{p_i}$ be the completion of $K$ at $p_i$. Let $m_i$ be the maximal ideal in the valuation ring $\mathcal{O}_i$ of an algebraic closure of $K_{p_i}$. For any $i \in \mathbb{Z}/\ell \mathbb{Z}^*$, we can consider $\mathcal{F}$ to be defined over $R_i = \mathbb{Z}[\zeta]_{p_i}$, in which case we can identify $\mathcal{F}(m_i)$ with the kernel of reduction of $J(\mathcal{O}_i)$ mod $m_i$.

By (5), for any $1 \leq i \leq g$ and any $\alpha \in p$, the isogeny $[\alpha]$ is not separable mod $p_i$, so $J(p^n)$ is in the kernel of reduction mod $m_i$ for any $n \geq 1$. Now fix any $i$, $1 \leq i \leq g$. For any $\alpha \in \mathbb{Z}[\zeta]$, let $\mathcal{F}[\alpha]$ denote the kernel of $\rho(\alpha)$ in $\mathcal{F}(m_i)$, and for any ideal $a \subseteq \mathbb{Z}[\zeta]$, let $\mathcal{F}[a] = \bigcap_{a \in \mathbb{Z}[\zeta] - \mathcal{F}(a)}$. Hence, for any $n \geq 1$ we can identify $J(p^n) = \mathcal{F}[p^n]$. Let $\pi \in \mathbb{Z}[\zeta]$ be a uniformizer at $p$ which is prime to all other conjugates of $p$. It is easy to see that

$$\mathcal{F}[p^n] = \mathcal{F}[\pi^n].$$

Indeed, the containment of the left-hand side of (6) in the right-hand side follows by definition, and since for any $a \leq b$, $(p^b, \pi^n) = p^n$, it suffices to show the reverse inclusion for those $n$ which are a multiple of the class number $h$ of $K$. However, if $(\alpha) = p^h$, then $\pi^h = \beta\alpha$, for some $\beta \in \mathbb{Z}[\zeta]$ prime to $p$, so $\rho(\beta)$ is an automorphism of $\mathcal{F}$ over $R_i$.

**Proof of Theorem 1.** We now assume that $p$ is a first or second degree prime and that $n \geq 1$. As above, fix an $i$, $1 \leq i \leq g$. Note that $\mathcal{F}[\pi^n]$ is precisely the set of solutions in $\mathcal{O}_i$ to the simultaneous equations

$$0 = \rho(\pi^n)_{j}(s_1, \ldots, s_g) = \sigma_j(\pi^n)s_j + (d^n \geq 2),$$

for $1 \leq j \leq g$. Since for any $1 \leq j \leq g$, $j \neq i$, $\sigma_j(\pi^n)$ is a unit in $R_i$, by the formal implicit function theorem (see, e.g., [Gra]), there are power series $\chi_j, j \neq i$, over $R_i$, without constant or linear term, such that the solutions to (7) are precisely the same as those of the system

$$s_j = \chi_j(s_i), j \neq i; V(s_i) = 0,$$

where $V$ is obtained by substituting $s_j = \chi_j(s_i)$ for all $j \neq i$ into the equation $0 = \rho(\alpha)_{i}(s_1, \ldots, s_g)$. Hence, $s_i$ takes on different values at every point of $J(p^n)$, and since it vanishes at the origin, for every $Q \in J(p^n)'$, we have $s_i(Q) \neq 0$. Since $\chi_j$ is without constant or linear term, $|s_i(Q)| > |s_j(Q)|$ for any $j \neq i$, where $| \cdot |$ denotes an absolute value on $\mathcal{O}_i$. Now pick any $1 \leq v \leq g$. Let $h_v = T_g^\ast P_v$, and let $c = [g + (1 - v)/2]$. Then by Proposition 2, the lead term in the expansion of $h_v$ at $0$ in terms $s_1, \ldots, s_g$, is of degree $d = [(v + 1)/2]$ and contains the monomial $\pm s_i^d$. Hence, $h_v(Q) \neq 0$, since taking $i = c$, there is a unique term in the expansion of $h_v(Q)$ in terms of $s_j(Q)$, $1 \leq j \leq g$, of maximal absolute value over $\mathcal{O}_i$.

Note that the divisor of $h_v$ is

$$v T_{(g+1)P}^\ast \Theta + T_{(g-v)P}^\ast \Theta - (v+1)T_{gP}^\ast \Theta.$$

Since $h_v(Q) \neq 0$,

$$Q \notin T_{(g-v)P}^\ast \Theta$$

for all $1 \leq v \leq g$. Since $\Theta$ is symmetric, replacing $Q$ by $-1|Q$ also gives (8) for $g + 1 \leq v \leq 2g - 1$. Finally, note that $Q \notin T_{gP}^\ast \Theta$, since the origin does not lie on $T_{gP}^\ast \Theta$ mod $m_i$, and $Q$ is in the kernel of reduction mod $m_i$. This shows that (8) also holds for $v = 0, 2g$, and gives us the theorem.

**Proof of Theorem 2.** Assume now that $p$ is a prime of $K$ of arbitrary residue degree $d$ that lies over the rational prime $p \neq \ell$. As above, fix an $i$, $1 \leq i \leq g$, and set $p_i = \sigma_i(p)$. It is now a seemingly hard problem in general to compute $|s_j(Q)|$ for some $1 \leq j \leq g$, $Q \in \mathcal{F}[p]^\prime$, and $| \cdot |$ an absolute value on $\mathcal{O}_i$. However, in [Gra] such a problem is solved under the assumptions that $\mathcal{F}$ has 'complex multiplication' by $\mathbb{Z}[\zeta]$ with CM-type $\Phi$ (i.e. (5) holds), that there is an $\alpha \in \mathbb{Z}[\zeta]$ such that $[\alpha]$ reduces to the Frobenius endomorphism of $\mathcal{F}$ mod $p_i$, with the factorization ($\alpha) = \prod_{\phi \in \Phi} \phi^{-1}(p_i)$ (which is just the congruence relation from the theory of complex multiplication of $\mathbb{Q}$).
Torsion on theta divisors of hyperelliptic Fermat Jacobians

abelian varieties), that $F[\phi^{-1}(p_i)^m] \cong \mathbb{Z}[\zeta]/\phi^{-1}(p_i)^m$ for every $m \geq 1$ and every $\phi \in \Phi$ (which follows since $J$ has full complex multiplication by $\mathbb{Z}[\zeta]$), and also that $F$ is a $p$-typical group (see [Haz78]), which $F$ is not.

However, as described in [Gra, § 2], there is a $p$-typical formal group $G$ over $R_i$ (called the ‘$p$-typification’ of $F$), and a strict isomorphism $\psi = (\psi_m)_{1 \leq m \leq g}$ over $R_i$ from $F$ to $G$, so that if $S_m, 1 \leq m \leq g$, are the parameters of $G$, then

$$S_m = \psi_m(s_1, \ldots, s_g) = s_m + (d^o \geq 2). \quad (9)$$

It follows from [Gra, Lemma 4] that $G$ is now a formal group over $R_i$ with complex multiplication by $\mathbb{Z}[\zeta]$ with CM-type $\Phi$, and it follows from the existence of $\psi$ that for the same $\alpha$ as for $F$, the endomorphism $[\alpha]$ on $G$ reduces to the Frobenius endomorphism of $G$ mod $p_i$, and that $G[\phi^{-1}(p_i)^m] \cong \mathbb{Z}[\zeta]/\phi^{-1}(p_i)^m$ for every $m \geq 1$ and every $\phi \in \Phi$. Hence, $G$ satisfies the hypotheses of [Gra, Proposition 1], whose conclusion gives us the following proposition.

**Proposition 3.** Let $\omega(r, j) \alpha$ and $E_{r, j}$ be as in the Introduction, and let $S_1, \ldots, S_g$ be the parameters for $G$. Let $w$ be the normalized $p_i$-adic valuation extended to $O_i$. Then for any $Q \in J[p]$, $w(S_{\omega(r,j)}(Q)) = (1/(p^l - 1))E_{r,j}$.

Hence, if $\omega(r, j')$ is admissible for $p$ and $Q \in J[p]'$, $w(S_{\omega(r,j')}(Q))$ is the unique minimal valuation among all $w(S_{\omega(r,j)}(Q)), j \in \mathbb{Z}/d_e \mathbb{Z}$. Furthermore, by [Gra, Remark 2], $w(S_{\omega(r,j')}(Q))$ is the unique minimal valuation among $w(S_m(Q))$ for all $1 \leq m \leq g$. So by (9), the same must be true for $w(S_{\omega(r,j')}(Q))$. Therefore, as in the proof of Theorem 1, if $[g + (1 - v)/2] = \omega(r, j')$, that is, if $g = g - v$ is good for $p$, then $h_v(Q) \neq 0$. We conclude as in (8) that $Q \notin T_{q^p}$. Again replacing $Q$ by $[1]Q$ shows that $Q \notin T_{q^p}$. Finally, by the same reason as in the proof of Theorem 1, $Q \notin T_{q^p}$. \hfill \Box

**Remark.** See [GS] for a complete determination of the torsion of $J$ that lies on $\phi(C)$.

**References**


David Grant grant@boulder.colorado.edu

Department of Mathematics, University of Colorado at Boulder, Boulder, CO 80309, USA