CUSPIDAL DIVISORS ON A FERMAT CURVE, FOLLOWING ROHRLICH

WILLIAM G. MCCALLUM

Let $p$ be an odd prime. Let $F$ be the curve $X^p + Y^p + Z^p = 0$. We call a point in $F(K)$ a cusp if one of its coordinates is zero. Let $J$ be the jacobian of $F$. Rohrlch [Roh77] studied the subgroup $T$ of $J(\mathbb{Q})$ generated by divisors of degree zero supported on the cusps. The purpose of this note is to reformulate Rohrlch’s results in terms of the endomorphism ring of $J$.

The action of the group $\mu_p$ of $p$-th roots of unity on each coordinate induces a faithful action of $G = \mu_p^p/\text{diag}$ on $F$, defined over $K$. There is also a natural action of the symmetric group $S_3$ on $F$ by permutation of the coordinates. The automorphism group of $F$ is a semi-direct product $G \rtimes S_3$, where the action of $S_3$ on $G$ is derived from its natural action on $\mu_p^p$. Let $R = \mathbb{Z}[\text{Aut}(F)]$ and let $I$ be the augmentation ideal in $R$. An easy computation shows that any divisor of degree zero supported on the cusps is killed by $p$ in the divisor class group. Thus

$$(1) \quad pIc \text{ is zero in } J.$$

Rohrlch found further relations among the cusps. Our first theorem below reformulates these relations in terms of the action of $R$ on $J$. Let $\Gamma_j$ be the image in $G$ of the $j$-th coordinate axis in $\mu_p^p$, let $\gamma_j$ be a generator of $\Gamma_j$, and let $\rho$ be a 3-cycle in $S_3$.

**Theorem 1.** Let $c$ be a cusp defined over $\mathbb{Q}$ and let $\gamma = \gamma_j$, for some $1 \leq j \leq 3$. Then the divisors of degree zero

$$(\gamma^\frac{1}{2} - \gamma^{-\frac{1}{2}})^{p-3}c, \quad (1-\rho) (\gamma^\frac{1}{2} - \gamma^{-\frac{1}{2}})^{p-2}c, \quad \text{and} \quad (1+\rho+\rho^2) (\gamma^\frac{1}{2} - \gamma^{-\frac{1}{2}})^{p-3}c$$

all represent 0 in $J$.

**Proof.** There are three cusps defined over $\mathbb{Q}$, cyclically permuted by $\rho$. Since conjugation by $\rho$ permutes the subgroups $\Gamma_j$, it suffices to prove the theorem for one of the cusps. Let $\zeta = e^{2\pi i/p}$. Following the notation of [Roh77], we denote the cusps

$$a_j = (0, \zeta^j, -1), \quad b_j = (\zeta^j, 0, -1), \quad c_j = (\zeta^j + \frac{1}{2p}, -1, 0), \quad 0 \leq j \leq p-1.$$

(Note that our coordinate $Z$ is the negative of Rohrlch’s.) We choose $c = a_0$. If $\gamma = \gamma_1$ then $\gamma$ fixes $c$ and the statement of the theorem is trivial. Since $\gamma_2$ and $\gamma_3$ act as inverses of each other on $c$, it suffices to prove the theorem for just one of them, say $\gamma_2$. We assume henceforth that $\gamma = \gamma_2$.

---

*Date: March 16, 2001.*
Let \( x = X/Z, y = Y/Z \). According to the table in [Roh77, p. 98], the function \( x/(y-1) \) has divisor

\[
\sum_{j=1}^{p-1} (a_j - a_0) = \sum_{j=1}^{p-1} \sum_{k=1}^{j-1} (a_k - a_{k-1}) = \left( \sum_{j=1}^{p-1} \sum_{k=0}^{j-1} \gamma^k \right) (a_1 - a_0)
\]

\[
= \left( \sum_{k=1}^{p-1} (p-1-k) \gamma^k \right) (a_1 - a_0)
\]

Since \( a_1 - a_0 = (\gamma - 1)a_0 \in Ia_0 \), we may, by (1), replace the coefficient of \( a_1 - a_0 \) in the above equation by anything congruent to it modulo \( p \). We have

\[
(1 - \gamma)^{p-2} = \sum_{k=0}^{p-2} (-1)^k \binom{p-2}{k} \gamma^k \equiv \sum_{k=0}^{p-2} (k+1) \gamma^k \equiv \sum_{k=1}^{p-1} (k+1) \gamma^k \pmod{p}.
\]

Thus \( (1 - \gamma)^{p-2} \) annihilates \( a_1 - a_0 \), hence \( (1 - \gamma)^{p-1} \) annihilates \( a_0 \). Thus

\[
(2) \quad (1 - \gamma)^{p-1} \text{ annihilates } a_0.
\]

Non-trivial relations. Rohrich discovered three non-obvious functions which give further relations between the cusps in the divisor class group. We will use

\[
a_j = \gamma^ja_0, \quad b_j = \rho^{-j}a_0, \quad c_j = \rho^2\gamma^j(p+1)/2a_0.
\]

The first relation is given by the function

\[
\frac{\left( \prod_{j=1}^{p-1} ((x - \zeta^j)(y - \zeta^j)^j) \right)^{1/p}}{(y-1)^{(p-1)/2}(x-1)^{(p-1)/2}},
\]

which has divisor

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

We have

\[
b_j - b_{j+1} = \rho \gamma^{-j-1}(a_1 - a_0)
\]

\[
b_j - b_0 = (b_j - b_{j+1}) + (b_{j+1} - b_{j+2}) + \cdots + (b_{p-1} - b_0)
\]

\[
= \rho(\gamma^{-j-1} + \gamma^{-j-2} + \cdots + \gamma^{-p})(a_1 - a_0)
\]

\[
= \rho \left( \sum_{k=j+1}^{p} \gamma^{-k} \right) (a_1 - a_0) = \rho \left( \sum_{k=j+1}^{p} \gamma^{p-k} \right) (a_1 - a_0).
\]

Thus

\[
\sum_{j=0}^{p-1} (j(a_j - a_0) + j(b_j - b_0)) = \left( \sum_{j=0}^{p-1} \sum_{k=0}^{j-1} \gamma^k + \rho \sum_{j=0}^{p-1} \sum_{k=0}^{p} \gamma^{p-k} \right)(a_1 - a_0)
\]

\[
= \sum_{k=0}^{p-1} \left( \sum_{j=k+1}^{p-1} j + \rho \sum_{j=0}^{p-k-1} j \right) \gamma^k (a_1 - a_0)
\]
The coefficient of $\gamma^k$ in this expression is congruent modulo $p$ to

$$-\sum_{j=1}^{k} j + \rho \sum_{j=0}^{p-k-1} j = -\frac{k(k+1)}{2} + \rho \frac{(p-k-1)(p-k)}{2} \equiv (\rho - 1) \frac{k(k+1)}{2}.$$ 

Furthermore,

$$\gamma^3 = \sum_{k=0}^{p-3} \gamma^k \left( \sum_{k=0}^{p-3} \frac{(k+1)(k+2)}{2} \gamma^{k-1} \right) \equiv \gamma^{-1} \sum_{k=0}^{p-1} \frac{k(k+1)}{2} \gamma^k.$$ 

Thus we conclude that $(\rho - 1)\gamma(1 - \gamma)^3$ annihilates $a_1 - a_0$, and hence that $(\rho - 1)\gamma(1 - \gamma)^3$ annihilates $a_0$. We can dispense with the lone $\gamma$ in the middle of this expression, since $(1 - \gamma)^{-1}$ annihilates $a_0$. Thus

$$\gamma^2 \left( (\rho - 1)(1 - \gamma)^{p-2} \right) \text{ annihilates } a_0.$$

We may multiply this element on the left by $\rho$ to obtain another element of the annihilator; this turns out to be equivalent to the second of Rohrlich’s nontrivial relations.

Finally, Rohrlich writes down a function which has divisor

$$\sum_{j=0}^{p-1} \frac{j(j+1)}{2} \left( (a_j - a_0) + (b_j - b_0) + (c_j - c_0) \right) =$$

$$\sum_{j=0}^{p-1} \frac{j(j+1)}{2} \left( \sum_{k=0}^{j-1} \gamma^k + \rho \sum_{k=j+1}^{p} \gamma^{p-k} + \rho^2 \sum_{k=j+1}^{p-1} \gamma^{k + \frac{k+1}{2}} \right) \gamma^k (a_1 - a_0) \equiv$$

$$\sum_{k=0}^{p-1} \left( -\frac{k}{2} + \rho \sum_{j=0}^{p-k-1} \frac{j(j+1)}{2} - \rho^2 \gamma^\frac{k+1}{2} \sum_{j=0}^{k} \frac{j(j+1)}{2} \right) \gamma^k (a_1 - a_0).$$

The coefficient of $\gamma^k$ in the sum is

$$-\frac{k(k+1)(k+2)}{6} + \rho \frac{(p-k-1)(p-k)(p-k+1)}{6} - \rho^2 \gamma^\frac{k+1}{2} \frac{k(k+1)(k+2)}{6} \equiv$$

$$-\frac{k(k+1)(k+2)}{6} - \rho \frac{(p-k-1)(k+1)}{6} - \rho^2 \gamma^\frac{k+1}{2} \frac{k(k+1)(k+2)}{6}.$$ 

Reasoning as before, we have

$$\gamma^4 \left( (\rho - 1)(1 - \gamma)^{p-4} \right) \text{ annihilates } a_0.$$
Therefore
\[
\frac{p-1}{k=0} \frac{k(k+1)(k+2)}{6} \gamma^k = \gamma(1-\gamma)^{p-4}
\]
\[
\frac{p-1}{k=0} \frac{(k-1)(k+1)}{6} \gamma^k = \gamma^2(1-\gamma)^{p-4}.
\]
So finally we get
\[(4) \quad (-\gamma - \rho \gamma^2 - \rho^2 \gamma^2 + \gamma^2 + \gamma^2)(1-\gamma)^{p-3} \in J.\]
The annihilators so far are:
\[pI, \quad (1-\gamma)^{p-1}, \quad (1-\rho)(1-\gamma)^{p-2}, \quad (\gamma + \rho \gamma^2 + \rho^2 \gamma^2 + \gamma^2 + \gamma^2)(1-\gamma)^{p-3}\]
The existence of the first as an annihilator means that we can multiply the second on the right by any power of $\gamma$. The existence of the second element and the others so obtained means that in the third element we can replace $1-\rho$ with $\gamma^a - \rho \gamma^b$ for any $a$ and $b$. This in turn means we can perform the following sort of move on the fourth element: pick any two of $1, \rho, \rho^2$, look at the powers of $\gamma$ that are the coefficients of those two, then increase one exponent by 1 and decrease the other exponent by 1. This means that we can replace the powers of $\gamma$ by any others as long as we preserve the sum of the exponents modulo $p$. Since the sum is currently $1 + 2 + (p + 3)/2 \equiv (3p + 9)/2$ modulo $p$, we can replace the fourth element by
\[(1 + \rho + \rho^2)\gamma^{\frac{p+5}{2}}(1-\gamma)^{p-3}.
\]
Now
\[\gamma^{\frac{p+5}{2}}(1-\gamma)^{p-3} = \gamma^{-\frac{p+1}{2}}(1-\gamma)^{p-3} = (\gamma^{\frac{3}{2}} - \gamma^{-\frac{3}{2}})^{p-3}.
\]
Also, the other annihilators may be freely multiplied on the right by any power of $\gamma$ and by $-1$. Thus, we may write the last three annihilators as
\[(\gamma^{\frac{3}{2}} - \gamma^{-\frac{3}{2}})^{p-1}, \quad (1-\rho)(\gamma^{\frac{3}{2}} - \gamma^{-\frac{3}{2}})^{p-2}, \quad (1 + \rho + \rho^2)(\gamma^{\frac{3}{2}} - \gamma^{-\frac{3}{2}})^{p-3},\]
as required. \qed

Since Aut($F$) is transitive on the cusps, any divisor of degree zero supported on the cusps may be written $rc$ for some $r \in I$. Thus the map $r \mapsto [rc]$ defines a surjective map $I \to T$. The kernel is a left ideal in $R$. For a subset $S \subset \mathbb{Z}[\mu_p]$, denote by $S^+$ the elements fixed under the involution $\zeta \mapsto \zeta^{-1}$. For a subgroup $H \subset$ Aut($F$), denote by $I[H]$ the augmentation ideal of $\mathbb{Z}[H]$. Rohrlich showed that the relations he discovered were the only ones; correspondingly, we can say that the annihilators in Theorem 1 are the only ones.

**Theorem 2.** Let $M \subset R$ be the left ideal
\[M = Ip + \sum_{j=1}^3 (RI(\Gamma_j)^{p-1} + R(1-\rho)I(\Gamma_j)^{p-2} + R(1 + \rho + \rho^2)(I(\Gamma_j)^{p-3})^+).
\]

Let $c \in C$ be a cusp defined over $\mathbb{Q}$ and let $H_c \subset$ Aut($F$) be the isotropy group of $c$. Then the map $c \mapsto rc$ induces an isomorphism of left $R$-modules
\[I/(RI(H_c) + M) \simeq T.
\]
Proof. Clearly, for any cusp \( c \), \( RI(H_c) \) annihilates \( c \). As before, it suffices to prove the theorem for \( c = a_0 \). Let \( \tau \in S_3 \) be the involution that fixes \( a_0 \). Then \( H_c = \Gamma_1 \rtimes \langle \tau \rangle \). Let \( \rho \) be the permutation \((XYZ)\). Then \( H_c, \gamma_2 \), and \( \rho \) generate \( \text{Aut}(F) \). Hence a \( \mathbb{Z} \)-basis for \( R/RI(H_c) \) is \( \{\rho^i \gamma_2^j \} \), \( 0 \leq i \leq 2 \), \( 0 \leq j \leq p - 1 \). It follows that \( I/(RI(H_c) + pI) \) is a \( \mathbb{Z}/p\mathbb{Z} \)-vector space of dimension \( 3p - 1 \). Let \( \pi = \gamma_2^{1/2} - \gamma_2^{-1/2} \). Then \( \pi \) is a generator of \( I(\Gamma_2) \) on which the involution \( \gamma \mapsto \gamma^{-1} \) acts by \(-1\). The image of \( M \) in \( I/(RI(H_c) + pI) \) is generated as an \( R \)-module by

\[
\pi^{p-1}, \quad (1 - \rho)\pi^{p-2}, \quad \text{and} \quad (1 + \rho + \rho^2)\pi^{p-3}.
\]

Since

\[
\pi^{p-1} = \alpha \rho + \beta (1 + \gamma + \cdots + \gamma^{p-1}),
\]

for some \( \alpha, \beta \in \mathbb{Z}[\gamma, \rho] \), we have \( (1 - \gamma)\pi^{p-1} \in pI \). Hence the submodule of \( I/(RI(H_c) + pI) \) generated by \( \pi^{p-1} \) is generated as a \( \mathbb{Z}/p\mathbb{Z} \)-vector space by \( \pi^{p-1} \), \( \rho \pi^{p-1} \), and \( \rho^2 \pi^{p-1} \), hence has dimension 3. Thus \( I/(RI(H_c), pI, \pi^{p-1}) \) has dimension \( 3p - 4 \). Finally, the submodule of this latter module generated by \( (1 - \rho)\pi^{p-2} \) and \( (1 + \rho + \rho^2)\pi^{p-3} \) has, as a \( \mathbb{Z}/p\mathbb{Z} \)-vector space, the basis \( (1 - \rho)\pi^{p-2}, (\rho - \rho^2)\pi^{p-2}, \) and \( (1 + \rho + \rho^2)\pi^{p-3} \). Hence \( I/(RI(H_c) + M) \) is has \( \mathbb{Z}/p\mathbb{Z} \)-rank \( 3p - 7 \). Since this is the same as the dimension of \( T \) computed by Rohrlich, and since, as we have already remarked, \( a_0 \) is clearly annihilated by \( I(H_c) \), it suffices to show that \( a_0 \) is annihilated by \( pI, \pi^{p-1}, (p - 1)\pi^{p-2}, \) and \( (1 + \rho + \rho^2)\pi^{p-3} \). This is what Theorem 1 tells us.

\[\square\]

References