# ALMOST RATIONAL TORSION POINTS AND THE CUSPIDAL TORSION PACKET ON FERMAT QUOTIENT CURVES

## PAVLOS TZERMIAS

#### 1. Introduction

Let  $\mathbb{Q}$  denote a fixed algebraic closure of the field  $\mathbb{Q}$  of rational numbers. Let p be a prime with  $p \geq 11$  and  $\zeta$  a primitive p-th root of 1 in  $\overline{\mathbb{Q}}$ . Let  $K = \mathbb{Q}(\zeta)$ . For  $a \in \{1, 2, ..., p-2\}$ , consider a smooth projective model  $F_{p,a}$  of the affine curve

$$v^p = u^a (1 - u).$$

The curves  $F_{p,a}$  are cyclic quotients of the Fermat curve of degree p and are called Fermat quotient curves. The curve  $F_{p,a}$  has genus (p-1)/2 and its Jacobian  $J_{p,a}$  admits complex multiplication by  $\mathbb{Z}[\zeta]$  which is induced by the automorphism  $\zeta : (u, v) \mapsto$  $(u, \zeta v)$  of  $F_{p,a}$ . By Section IV in [4], we know that the curve  $F_{p,a}$  is hyperelliptic if and only if  $a \in \{1, (p-1)/2, p-2\}$ . We will denote by S the set of values of a such that  $1 \leq a \leq p-2$  and  $F_{p,a}$  is not hyperelliptic. The cusps on  $F_{p,a}$  are the elements of the set  $C_{p,a} = \{(0,0), (1,0), \infty\}$ . Since the divisors of the rational functions u and 1-u are  $p((0,0)-\infty)$  and  $p((1,0)-\infty)$ , respectively, it follows that the difference of two points in  $C_{p,a}$  is a torsion point on  $J_{p,a}$  (we refer the reader to the work of Gross and Rohrlich in [9], where some deep related results are proven). For the rest of this paper, we fix a cusp c and the Albanese embedding of  $F_{p,a}$  in  $J_{p,a}$  given by  $P \mapsto [P-c]$ . The cuspidal torsion packet on  $F_{p,a}$  is the set  $T_{p,a} = F_{p,a} \cap (J_{p,a})_{\text{tors}}$ , whose elements are called cuspidal torsion points. By the Manin-Mumford conjecture (first proved by Raynaud in [14]),  $T_{p,a}$  is a finite set.

The purpose of this paper is to establish the following theorem:

**Theorem 1.1.** Let p be a prime such that  $p \ge 11$  and let  $a \in S$ . Then

$$T_{p,a} = C_{p,a}.$$

It was proven by Coleman, Tamagawa and the author in [6] that Theorem 1.1 is valid for certain a under certain conditions on p related to Vandiver's conjecture. Although the results of [6] were strong enough to establish the analogue of Theorem 1.1 for any Fermat curve of degree at least 4, the problem for the Fermat quotient curves remained open in general, since the Vandiver-type restrictions given in [6] were difficult to remove. The analogue of Theorem 1.1 for the hyperelliptic Fermat quotients was proven by Grant and Shaulis in [7]. Their method utilized the powerful theory of almost rational points introduced by Ribet (see [15] and [2] for a good account of the theory and its numerous ramifications). In this paper, which has been

Received by the editors August 18, 2004.

<sup>2000</sup> Mathematics Subject Classification. Primary 11G10, 11G30; Secondary 14K12.

Key words and phrases. Almost rational torsion, cuspidal torsion packet, Fermat quotients.

largely inspired by [2], [3], [6] and [7], we prove Theorem 1.1 by using Ribet's theory in conjunction with some of the results in [3], [6] and [7]. In the process, we also obtain partial results on the set of almost rational torsion points on  $J_{p,a}$  (see Section 3 below).

For the case of modular curves, the analogue of Theorem 1.1 was conjectured by Coleman, Kaskel and Ribet in [5]; it was established by Baker ([1]) and, independently, by Tamagawa ([16]). New proofs of the Manin-Mumford conjecture, the Coleman-Kaskel-Ribet conjecture and some of Tamagawa's results are given in [2].

#### 2. Galois action on torsion points

From now on, fix  $p \ge 11$  and  $a \in S$ . We write F instead of  $F_{p,a}$  and J instead of  $J_{p,a}$ . Let  $\lambda$  denote the endomorphism of J given by  $\lambda = \zeta - 1$ . Also, let A be the ring of integers in K and let  $A_p$  be its completion at the prime above p. We denote by M the maximal ideal of  $A_p$ . The element  $\lambda \in M$  is a uniformizer for  $A_p$ . Combining results of Coleman ([4]), Greenberg ([8]), Gross-Rohrlich ([9]) and Kurihara ([10]), we get that

(1)  $J(\mathbb{Q})_{\text{tors}} = J[\lambda],$ 

(2)  $J(K)_{\text{tors}} = J[\lambda^3]$ . In particular,  $J[l^{\infty}](K) = \{0\}$ , for primes l with  $l \neq p$ .

Let  $\Phi_a$  be the reflex type of the CM type of J with respect to A (see [13]) given by

$$\Phi_a = \sum_{t=1}^{p-1} (r(t) - 1)\sigma_{-t}^{-1},$$

where  $r(t) = \langle at/p \rangle + \langle t/p \rangle + \langle -(1+a)t/p \rangle$ ,  $\langle x \rangle$  denotes the fractional part of the real number x and  $\sigma_t$  is the element of  $\operatorname{Gal}(\mathbb{Q}_p(\zeta)/\mathbb{Q}_p) = \operatorname{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  defined by  $\sigma_t(\zeta) = \zeta^t$ . Observe that  $r(t) - 1 \in \{0, 1\}$ , for all t. Since r(t) + r(p-t) = 3, we get that r(t) - 1 = 1, for exactly (p-1)/2 values of  $t \in \{1, \dots, p-1\}$  and that r(t) - 1 = 1 if and only if r(p-t) - 1 = 0. Let X be the set of all  $t \in \{1, \dots, p-1\}$  such that r(t) - 1 = 1. It follows that for  $t, s \in X$ , we have  $t^2 \equiv s^2 \pmod{p}$  if and only if t = s. Also note that

$$\sigma_{-t}^{-1}(\lambda) \equiv -t^{-1}\lambda \pmod{\lambda^2},$$

 $\mathbf{SO}$ 

$$\sigma_{-t}^{-1}(\lambda^m) \equiv (-t^{-1})^m \lambda^m \pmod{\lambda^{m+1}},$$

for all  $m \ge 1$ . The following proposition is in the spirit of Lang ([12]) and Coleman-Kaskel-Ribet ([5]):

**Proposition 2.1.** Let m be an integer such that  $m \ge 2$  and

$$\sum_{t \in X} t^{-m} \not\equiv 0 \pmod{p}.$$

Then m is either odd or divisible by p-1 and there exist  $\tau \in Gal(K(J[p^{\infty}])/K)$  and  $r \in \mathbb{Z}_p[\zeta]^{\times}$  such that

$$\tau(y) = (1 + r\lambda^m)y,$$

for all  $y \in J[p^{\infty}]$ .

*Proof.* Suppose that m is not divisible by p-1. As explained before, the set  $\{t^2:$  $t \in X$  is a complete set of non-zero quadratic residues (mod p). Therefore, if m is even, then

$$\sum_{t \in X} t^{-m} = \sum_{i=1}^{(p-1)/2} i^{-m} = \frac{1}{2} \sum_{i=1}^{p-1} i^{-m} \equiv 0 \pmod{p},$$

a contradiction. So m is odd. Now, exactly as in the proof of Proposition 2 in [6], it suffices to show that there exists  $x \in 1 + M^2$  such that

$$x^{-\Phi_a} = 1 + s\lambda^m + \gamma,$$

where  $s \in \mathbb{Z}_p[\zeta]^{\times}$  and  $\gamma \in M^{m+1}$  (if this is the case, then we can set  $r = s + \gamma \lambda^{-m}$ ). Now let  $x = 1 + \lambda^m$ . Then

$$x^{-\Phi_a} \equiv \prod_{t \in X} (1 + (-1)^{m+1} t^{-m} \lambda^m) \equiv 1 + (-1)^{m+1} \left(\sum_{t \in X} t^{-m}\right) \lambda^m \pmod{\lambda^{m+1}},$$
  
d this is what we wanted to show.

and this is what we wanted to show.

We will also need the following easy lemma:

**Lemma 2.2.** If Y is a set of (p-1)/2 consecutive positive integers, then some  $m \in Y$ satisfies

$$\sum_{t\in X}t^{-m}\not\equiv 0\pmod{p}$$

*Proof.* If this is not the case, then the system of (p-1)/2 equations in (p-1)/2unknowns  $y_1, y_2, \cdots, y_{(p-1)/2}$  given by

$$\sum_{t_i \in X} t_i^{-m} y_i \equiv 0 \pmod{p},$$

where  $m \in Y$ , has the non-trivial solution  $(1, \dots, 1)$ . The determinant of the coefficient matrix is a non-zero multiple of a non-zero Vandermonde determinant  $(\mod p)$ , so it is non-zero  $(\mod p)$ , and this is a contradiction. 

#### 3. Almost rational torsion points

Following Ribet, we call a point  $D \in J(\overline{K})$  almost rational over K if, for all  $\sigma, \tau \in \operatorname{Gal}(\overline{K}/K)$ , the relation  $\sigma(D) + \tau(D) = 2D$  implies  $\sigma(D) = \tau(D) = D$ . Note that, since F is not hyperelliptic, its gonality exceeds 2, therefore the image of every point of  $F(\overline{K})$  in  $J(\overline{K})$  is almost rational. Now let  $\Sigma$  denote the set of torsion points on J which are almost rational over K.

**Lemma 3.1.** Let *l* be a prime and  $\delta$  a positive integer.

(1) 
$$J(K(J[l^{\delta}])) \cap J[l^{\infty}] = J[l^{\delta}].$$

(2) If l = p and m is an integer such that  $m \ge 2$  and

$$\sum_{x \in X} t^{-m} \not\equiv 0 \pmod{p},$$

then

$$J(K(J[\lambda^m])) \cap J[p^{\infty}] = J[\lambda^m]$$

Proof. (1) There exists  $\tau \in \operatorname{Gal}(K(J[l^{\infty}])/K)$  which acts on the *l*-adic Tate module of J as multiplication by  $1 + l^{\delta}$ . For l = p, this follows from observing that the proof of Proposition 2 in [6] (for 1 + p) also works for  $1 + p^{\delta}$ ; for  $l \neq p$ , this follows from Lemma 3.3 in [7] (we should point out that, although Lemma 3.3 in [7] is only stated for the hyperelliptic Fermat quotients, the same proof makes it valid for all Fermat quotients). Let  $D \in J(K(J[l^{\delta}])) \cap J[l^{\infty}]$ . Then  $\tau(y) = y$ , for all  $y \in J[l^{\delta}]$ , so  $\tau$  fixes  $K(J[l^{\delta}])$ , hence it also fixes  $J(K(J[l^{\delta}]))$ . In particular,  $\tau(D) = D$ , so  $l^{\delta}D = 0$ , i.e.  $D \in J[l^{\delta}]$ . The reverse inclusion is obvious.

(2) Suppose that  $D \in J(K(J[\lambda^m])) \cap J[p^{\infty}]$ . Choose  $\tau$  as in Proposition 2.1. Then  $\tau(y) = y$ , for all  $y \in J[\lambda^m]$ , so  $\tau$  fixes  $K(J[\lambda^m])$ , hence it also fixes  $J(K(J[\lambda^m]))$ . In particular,  $\tau(D) = D$ , therefore,  $r\lambda^m D = 0$ . Since r is invertible in  $\mathbb{Z}_p[\zeta]$ , it follows that  $D \in J[\lambda^m]$ . The reverse inclusion is obvious.

**Proposition 3.2.** Let *l* be a prime. Let  $\delta = 1$ , for *l* odd, and  $\delta = 2$ , for l = 2.

- (1)  $\Sigma \cap J[l^{\infty}] \subseteq J[l^{\delta}]$ . If, in addition,  $l \neq 3, p$ , then  $\Sigma \cap J[l^{\infty}] = \{0\}$ .
- (2) If l = p, let m be the smallest integer in  $\{(p-1)/2, \dots, p-2\}$  such that

$$\sum_{t\in X}t^{-m}\not\equiv 0\pmod{p}$$

(such *m* exists, by Lemma 2.2). Then  $\Sigma \cap J[p^{\infty}] \subseteq J[\lambda^m]$ . In particular, if  $p \equiv 3 \pmod{4}$ , then  $\Sigma \cap J[p^{\infty}] \subseteq J[\lambda^{(p-1)/2}]$ .

*Proof.* (1) The first assertion follows by combining Proposition C in [3] (with  $\Omega = \{l\}$  and  $L = l^{\delta}$ ) and Part (1) of Lemma 3.1.

Now suppose that  $l \neq 3, p$  and l is odd. Then both (1+l)/2 and (3+l)/2 are units in  $\mathbb{Z}_l$ . By Lemma 3.3 in [7], we can find  $\sigma, \tau \in \text{Gal}(K(J[l^{\infty}])/K)$  acting as the homotheties (1+l)/2, (3+l)/2 on the *l*-adic Tate module of *J*. If *D* is a non-trivial *l*-torsion point on *J*, it follows that

$$\sigma(D) + \tau(D) = \frac{1+l}{2}D + \frac{3+l}{2}D = 2D.$$

However  $\sigma(D) \neq \tau(D)$ , so  $D \notin \Sigma$ .

Next suppose that l = 2. Let D be a non-trivial 4-torsion point on J. Since  $p \ge 11$ , we see that D is not K-rational (by (2) at the beginning of Section 2). If the order of D equals 2, choose  $\sigma \in \text{Gal}(K(J[2^{\infty}])/K)$  such that  $\sigma(D) \ne D$ . Since

$$\sigma(D) + \sigma(D) = \sigma(2D) = 0 = 2D,$$

D is not in  $\Sigma$ . If the order of D equals 4, choose, again by Lemma 3.3 in [7],  $\sigma \in \text{Gal}(K(J[2^{\infty}])/K)$  acting as the homothety 3 on the 2-adic Tate module of J. Then  $\sigma(D) + \sigma(D) = 2D$ , but  $\sigma(D) \neq D$ , so  $D \notin \Sigma$ .

(2) Let  $D \in \Sigma \cap J[p^{\infty}]$ . By Part (1), we get that  $D \in J[p] = J[\lambda^{p-1}]$ . Let  $\sigma$  be any element of  $\operatorname{Gal}(K(J[p^{\infty}])/K(J[\lambda^m]))$ . We claim that  $\sigma(D) = D$ . Note that  $\lambda^m D \in J[\lambda^{p-1-m}]$ . Since  $\sigma$  fixes  $K(J[\lambda^m])$  and  $p-1-m \leq m$ , it follows that  $\sigma$  fixes  $J[\lambda^{p-1-m}]$ , so it fixes  $\lambda^m D$ . Since  $\sigma$  commutes with  $\lambda$ , it follows that  $\sigma(D) - D \in J[\lambda^m]$ . But then  $\sigma(D) - D$  is fixed by  $\sigma$ , i.e.  $\sigma^2(D) + D = 2\sigma(D)$ . Since D is almost rational over K, so is  $\sigma(D)$ , therefore  $\sigma(D) = D$ , and this proves the claim. This holds for all  $\sigma$  fixing  $K(J[\lambda^m])$ , so D is defined over the latter field, i.e.  $D \in J(K(J[\lambda^m]))$ . By Part (2) of Lemma 3.1, we get  $D \in J[\lambda^m]$ . In particular,

suppose that  $p \equiv 3 \pmod{4}$ . Then (p-1)/2 is odd and  $t^{(p-1)/2} = \pm 1$ , for all  $t \in X$ . This shows that m = (p-1)/2 in this case.

### 4. The cuspidal torsion packet

We are now ready to prove Theorem 1.1. Note that, by Theorem 9 in [4], all cuspidal torsion points are of p-power order. By the first paragraph of Section 3, they are also almost rational over K.

Suppose that  $p \equiv 3 \pmod{4}$ . By Part (2) of Proposition 3.2, we see that the cuspidal torsion packet is contained in  $F \cap J[\lambda^{(p-1)/2}]$ . By Proposition 3 in [6], we have  $\sharp(F \cap J[\lambda^{(p-1)/2}]) \leq p(p-1)/2$ . If there exists a point in  $F \cap J[\lambda^{(p-1)/2}]$  which is not K-rational, then, by [8], its field of definition over K has degree at least p, hence, by Lemma 2 in [6], we have  $\sharp(F \cap J[\lambda^{(p-1)/2}]) \geq p^2$ , and this is a contradiction. Therefore,  $F \cap J[\lambda^{(p-1)/2}] \subseteq J[\lambda^3]$ . By Proposition 4 in [6], it follows that

$$F \cap J[\lambda^{(p-1)/2}] \subseteq F \cap J[\lambda] = \{(0,0), (1,0), \infty\},\$$

where the latter equality follows from the proof of Theorem 3 in [6], and this proves the assertion. This is not a new result; the same result is also obtained in [6] (see the Remark following Theorem 3 in [6]).

Now suppose that  $p \equiv 1 \pmod{4}$  and let P be a cuspidal torsion point on F. If  $P \in J[\lambda^{(p-1)/2}]$ , we are done by the same proof as in the case of  $p \equiv 3 \pmod{4}$ . So, assume  $P \notin J[\lambda^{(p-1)/2}]$  (note that then P is not K-rational by (2) at the beginning of Section 2). Then  $P \in J[\lambda^k]$  and  $P \notin J[\lambda^{k-1}]$  hold for some k with  $(p-1)/2 < k \leq m$ , where m is as in Part (2) of Proposition 3.2. If the field of definition K(P) of P over K does not equal  $K(J[\lambda^4])$ , then, by [8] and (2) at the beginning of Section 2, we have  $[K(P) : K(J[\lambda^4])] \geq p$  and  $[K(J[\lambda^4]) : K] \geq p$ , hence  $[K(P) : K] \geq p^2$ . We can therefore apply Lemma 2 in [6] and get  $\#(F \cap J[p]) \geq p^3$ , contradicting Proposition 2 in [6]. So suppose that  $K(P) = K(J[\lambda^4])$ . Then, since P generates  $J[\lambda^k]$  as a  $\mathbb{Z}[\lambda]$ -module, we get

$$K(J[\lambda^k]) = K(J[\lambda^{k-1}]) = \dots = K(J[\lambda^4]).$$

We consider two cases:

Case 1. Suppose that  $k \ge 4 + (p-1)/2$ . Then, since *m* must be odd (by Proposition 2.1), we get  $m \ge 5 + (p-1)/2$ . By Lemma 2.2 and the minimality of *m*, there exists *n* such that  $5 \le n < (p-1)/2$  such that

$$\sum_{t \in X} t^{-n} \not\equiv 0 \pmod{p}.$$

Now let  $\sigma$  be a Galois automorphism fixing  $K(J[\lambda^n])$ . Note that  $\lambda^n P \in J[\lambda^{k-n}]$ . Since  $n \geq 5$ ,  $k - n \geq 4$ , we get  $K(J[\lambda^{k-n}]) = K(J[\lambda^n])$ , so  $\sigma$  fixes  $\lambda^n P$ , therefore  $\sigma(P) - P \in J[\lambda^n]$ . But then  $\sigma(P) - P$  is fixed by  $\sigma$ , hence, by almost rationality of P, it follows that P is fixed by  $\sigma$ . This works for all  $\sigma$  fixing  $K(J[\lambda^n])$ , which implies that  $P \in J(K(J[\lambda^n]))$ . By Part (2) of Lemma 3.1, we have

$$J(K(J[\lambda^n])) \cap J[p^{\infty}] \subseteq J[\lambda^n],$$

from which it follows that  $P \in J[\lambda^n]$ , a contradiction.

Case 2.  $(p-1)/2 < k \leq 3 + (p-1)/2$ . Let  $b = k - (p-1)/2 \in \{1, 2, 3\}$ . The following arguments were obtained jointly with Coleman and Tamagawa during our collaboration in [6] (see also the last paragraph of Section 1 in [6]).

**Lemma 4.1.** Suppose that b = 2 or 3. Let G be the semidirect product of  $Gal(K/\mathbb{Q})$ and  $Gal(K(P)/K) \times \mu_p$  with the natural action of the former group on the latter. Then P has at least  $p^2(p-1)/4$  G-conjugates.

Proof. The proof is very similar to the proof of Proposition 4 in [6]. Let H be the stabilizer of P in G. By the proof of Lemma 2 in [6], no element of  $\operatorname{Gal}(K(P)/K) \times \mu_p$  fixes P. Therefore H embeds into  $\operatorname{Gal}(K/\mathbb{Q})$ . Let  $\sigma \in H$ . Suppose that  $\sigma(\zeta) = \zeta^{\beta}$ . Since the point  $R = \lambda^{b+(p-3)/2}P \in J[\lambda] \setminus \{0\}$  is defined over  $\mathbb{Q}$ , we get  $\beta^{b+(p-3)/2}R = R$ , so the order of  $\beta$  divides both b + (p-3)/2 and p-1. This means that the order of  $\beta$  divides 4, so the image of H in  $\operatorname{Gal}(K/\mathbb{Q})$  is of order at most 4. This proves the assertion, because  $\sharp(G) = p^2(p-1)$ .

**Lemma 4.2.** Let W be the theta divisor of J. Consider the following endomorphisms of J:

$$\tau = \prod_{i=1}^{(p-1)/2} (\zeta^i - \zeta^{-i}), \quad a_1 = \tau\lambda, \quad a_2 = \tau\lambda(\zeta^2 - 1), \quad a_3 = \tau\lambda(\zeta^2 - 1)(\zeta^3 - 1).$$

Let (·) denote the intersection pairing between 1-cycles and (p-3)/2-cycles on J modulo rational equivalence.

(1)  $(F \cdot a_1^{-1}(W)) = p^2$ . (2)  $(F \cdot a_2^{-1}(W)) = 2p^2$ . (3)  $(F \cdot a_3^{-1}(W)) = 3p^2$ .

*Proof.* Since  $a_i \in \mathbb{Z}[\zeta]$ , for all *i*, it follows from Chapter V, § 3, D4, D8 and Chapter IV, § 3, Corollary to Theorem 7 in [11] that

$$(F \cdot a_i^{-1}(W)) = \operatorname{Trace}_{K^+/\mathbb{Q}}(\operatorname{Norm}_{K/K^+}(a_i))$$

for all i, where  $K^+$  is the maximal real subfield of K. Lemma 4.2 now follows from a simple calculation.

Now, if b = 2 or 3, then, by Lemma 4.1, P has at least  $p^2(p-1)/4$  G-conjugates. On the other hand, by Parts (2) and (3) of Lemma 4.2 and the proof of Proposition 3 in [6], we get  $\sharp(F \cap J[\lambda^k]) \leq 3p^2$ . Taking into account the three  $\mathbb{Q}$ -rational cusps, this gives  $3 + p^2(p-1)/4 \leq 3p^2$ , which is impossible, since  $p \geq 13$ .

If b = 1, then, by Lemma 2 in [6], P has at least  $p^2$  conjugates over K. Taking into account the three  $\mathbb{Q}$ -rational cusps, this gives  $\sharp(F \cap J[\lambda^k]) \ge p^2 + 3$ . By the proof of Proposition 3 in [6], this contradicts Part (1) of Lemma 4.2.

#### Acknowledgements

I heartily thank Robert Coleman and Akio Tamagawa for our valuable discussions during our collaboration on [6]. The arguments needed to handle a special case of our proof (see Lemmas 4.1 and 4.2 above) were obtained jointly with them. I am also indebted to the anonymous referee for his/her careful reading and constructive criticism of a previous version of the paper.

#### References

- [1] M. Baker, Torsion points on modular curves, Invent. Math. 140 (2000), no. 3, 487–509.
- [2] M. Baker and K. Ribet, Galois theory and torsion points on curves, J. Théor. Nombres Bordeaux 15 (2003), no. 1, 11–32.
- [3] J. Boxall and D. Grant, Singular torsion points on elliptic curves, Math. Res. Lett. 10 (2003), no. 5-6, 847-866.
- [4] R. Coleman, Torsion points on abelian étale coverings of P<sup>1</sup> − {0,1,∞}, Trans. Amer. Math. Soc. **311** (1989), no. 1, 185–208.
- [5] R. Coleman, B. Kaskel, and K. Ribet, Torsion points on X<sub>0</sub>(N), Proc. Sympos. Pure Math. 66 (1999), no. 1, 27–49.
- [6] R. Coleman, A. Tamagawa, and P. Tzermias, The cuspidal torsion packet on the Fermat curve, J. Reine Angew. Math. 496 (1998) 73–81.
- [7] D. Grant and D. Shaulis, The cuspidal torsion packet on hyperelliptic Fermat quotients, J. Théor. Nombres Bordeaux 16 (2004), no. 3, 577–585.
- [8] R. Greenberg, On the Jacobian variety of some algebraic curves, Compositio Math. 42 (1981) 345–359.
- 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.
- [10] M. Kurihara, Some remarks on conjectures about cyclotomic fields and K-groups of Z, Compositio Math. 81 (1992) 223–236.
- [11] S. Lang, Abelian varieties, Interscience Publishers (1959).
- [12] —, Division points on curves, Ann. Mat. Pura Appl. 70 (1965) 229–234.
- [13] ——, Complex Multiplication, Vol. 255, Springer-Verlag, New York (1983).
- [14] M. Raynaud, Courbes sur une variété abélienne et points de torsion, Invent. Math. 71 (1983) 207–233.
- [15] K. Ribet and M. Kim, Torsion points on curves and Galois theory, Notes of a series of talks by K. Ribet in the Distinguished Lecture Series, Southwestern Center for Arithmetic Algebraic Geometry (1999)
- [16] A. Tamagawa, Ramification of torsion points on curves with ordinary semistable Jacobian varieties, Duke Math. J. 106 (2001), no. 2, 281–319.

Department of Mathematics, University of Tennessee, Knoxville, TN 37996-1300  $E\text{-}mail\ address: \texttt{tzermias@math.utk.edu}$