

LOW-DEGREE POINTS ON HURWITZ-KLEIN CURVES

PAVLOS TZERMIAS

ABSTRACT. We investigate low-degree points on the Fermat curve of degree 13, the Snyder quintic curve and the Klein quartic curve. We compute all quadratic points on these curves and use Coleman's effective Chabauty method to obtain bounds for the number of cubic points on each of the former two curves.

1. INTRODUCTION

Let \mathbb{Q} be the field of rational numbers and let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of \mathbb{Q} . For a curve C of genus $g \geq 2$ defined over \mathbb{Q} , let J denote the Jacobian of C . Assuming that C has a \mathbb{Q} -rational point P_0 , we fix an Albanese embedding of C in J by choosing P_0 as a base point. For a positive integer d , let W_d denote the image of the d -th symmetric power $C^{(d)}$ of C in J under the map induced by the fixed Albanese embedding of C in J . Recall that the gonality γ of C is defined as the smallest degree of a morphism from C to \mathbb{P}^1 . Let us recall the following special case of a celebrated theorem of Faltings ([7]):

Theorem 1.1 (Faltings). *If $d < \gamma$ and W_d does not contain a translate of a non-trivial abelian subvariety of J , then there are only finitely many $\overline{\mathbb{Q}}$ -points on C whose field of definition has degree at most d over \mathbb{Q} .*

We refer to such points as low-degree points on C . In the case of a smooth plane curve C of degree $N \geq 7$, Debarre and Klassen ([5]) have shown that the conclusion of the above theorem holds for $d \leq N - 2$. Explicit versions of such results for specific curves are hard to obtain. In this paper, we will be concerned with two special types of curves, namely the Fermat curves and the Hurwitz-Klein curves whose definition we now recall:

Let p be a fixed prime, such that $p \geq 5$. We denote by F_p the Fermat curve of degree p , i.e. the complete plane curve over \mathbb{Q} given by the projective equation

$$X^p + Y^p + Z^p = 0.$$

Suppose that, in addition, $p \equiv 1 \pmod{3}$. Let $F_{p,r}$ denote a smooth projective model of the singular affine curve

$$y^p = x^r(1-x),$$

where r is a primitive cube root of unity \pmod{p} . It was observed by Lefschetz ([13]) that $F_{p,r}$ has a cubic automorphism ρ . Note that $F_{p,r}$ arises as a quotient of F_p

Received by the editors January 31, 2001 and, in revised form, August 1, 2001 and May 31, 2002.

2000 *Mathematics Subject Classification*. Primary 11G30, 14H25; Secondary 11G10, 14G05.

Key words and phrases. Hurwitz-Klein curves, Fermat curves, low-degree points.

by a certain group of automorphisms of F_p (see [8]). Also the Jacobian $J_{p,r}$ of $F_{p,r}$ has complex multiplication by a primitive p -th root of unity ζ in $\overline{\mathbb{Q}}$. Let K denote the cyclotomic field $\mathbb{Q}(\zeta)$. It is well known from the work of Hurwitz ([9]) that $F_{p,r}$ is also given by the (singular) model

$$x^m y^n + y^m + x^n = 0,$$

where m and n are positive integers such that $m^2 - mn + n^2 = p$ (the existence of such integers follows from the fact that p splits completely in $\mathbb{Q}(\sqrt{-3})$). In this model, the cubic automorphism of $F_{p,r}$ is given by $\rho(x, y) = (1/y, x/y)$. Both models of $F_{p,r}$ will be used in this paper. We will refer to $F_{p,r}$ as a Hurwitz-Klein curve. Two of these curves, namely $F_{7,2}$ (the Klein quartic) and $F_{13,3}$ (the Snyder quintic), will be extensively studied in this paper.

While all \mathbb{Q} -rational points on F_p are now known thanks to Wiles and Taylor ([21], [18]), analogous results for low-degree points on F_p have only been obtained in special cases. Gross and Rohrlich ([8]) computed all points of degree at most $(p-1)/2$ on F_p for $p \leq 11$. Debarre and Klassen ([5]) asked whether all points of degree at most $p-2$ on F_p lie on the line $X+Y+Z=0$ (for all $p \geq 5$). A similar question has been raised by Ribenboim ([17]). The former question has been settled affirmatively for $p=5$ ([10]) and for $p=7$ ([19]). The points of degree at most 5 on F_{11} have been computed by Gross and Rohrlich in [8]. Also the main result of [20] is that there are at most 120 points of degree 6 on F_{11} . A closer look at the latter results and their proofs leads to the following observation: in all the known cases, the $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -orbit of a low-degree point R on F_p is contained in the S_3 -orbit of R , where we identify S_3 with the obvious subgroup of the automorphism group of F_p . In this paper we verify part of the same assertion for $p=13$. Our main result is as follows:

Theorem 1.2. *There are exactly 3 rational points, 2 quadratic points and at most 27 cubic points on F_{13} . Moreover, the Galois orbit of any of these points is contained in its S_3 -orbit.*

We of course claim no novelty for the result about rational points; we have included it in the statement of the above theorem only for the sake of completeness. To our knowledge, the result about quadratic and cubic points is the first example of a result of this type for a Fermat curve whose Jacobian conjecturally has no Faddeev factor (i.e. a factor of the form $J_{p,r}$) with finite Mordell-Weil group (the predictions of the Birch and Swinnerton-Dyer conjecture regarding Mordell-Weil ranks of Fermat Jacobians are discussed in [8]). The proof of Theorem 1.2 uses the geometry of $J_{13,3}$ (studied by Lim in [14]), Coleman's effective Chabauty bound ([2]) and a technical device (Theorem 1.3 below) which is valid only under a strong (and difficult to settle in general) Mordell-Weil rank condition. Following Lim ([14]), let C_0 denote the quotient of $F_{p,r}$ by the group of automorphisms generated by ρ . Let J_0 denote the Jacobian of C_0 . Note that the Mordell-Weil ranks of J_0 and $J_{p,r}$ over \mathbb{Q} satisfy $\text{rk}(J_0(\mathbb{Q})) \leq \text{rk}(J_{p,r}(\mathbb{Q}))$. The technical device mentioned above is the following theorem:

Theorem 1.3. *Suppose that $\text{rk}(J_0(\mathbb{Q})) \geq \text{rk}(J_{p,r}(\mathbb{Q})) - 1$. Then there are exactly 3 rational points and 2 quadratic points on $F_{p,r}$. In particular, if the above rank condition is satisfied, there are exactly 3 rational points and 2 quadratic points on F_p .*

The fact that $F_{p,r}$ has exactly 3 rational points for all p and r (unconditionally) follows from the work of Wiles and Taylor ([21], [18]). We should therefore point out that we include a statement about rational points in Theorem 1.3 only for the sake of completeness. Also the Mordell-Weil rank condition in Theorem 1.3 is a strong restriction. By Corollary 2.2 in the next section, it is always satisfied if $\text{rk}(J_{p,r}(\mathbb{Q})) \leq 2$ and, in particular, for $p = 7$ and $p = 13$. For the case $p = 7$, we thus obtain a generalization of the classical theorem of Hurwitz in [9] (see also [3] for a different proof by Coleman) describing the rational points on the Klein quartic. We should also point out that the determination of the quadratic points on $F_{7,2}$ also follows from the work of Gross and Rohrlich in [8], as shown in the Ph.D. thesis of Oumar Sall. In the next section we discuss the Mordell-Weil rank condition of Theorem 1.3 in more detail (see in particular the remark following Corollary 2.2). Joint work in progress with William McCallum may provide some answers regarding the extent to which it might be true more generally.

Remark. The computation of all rational and quadratic points on the curves $F_{7,2}$ and $F_{13,3}$ easily provides similar results for curves which cover one of them over \mathbb{Q} . The example of Hurwitz-Klein curves of the form $X^m Y + Y^m Z + Z^m X = 0$, where $m \geq 3$ is an integer such that $m \equiv 3 \pmod{7}$ or $m \equiv 5 \pmod{7}$ or $m \equiv 4 \pmod{13}$ or $m \equiv 10 \pmod{13}$, is discussed in section 3 (see the remark at the end of that section).

2. THE GEOMETRY OF $J_{p,r}$

Following the notation of Theorem 1.3, p is a prime such that $p \equiv 1 \pmod{3}$ and r is a primitive cube root of unity \pmod{p} . Recall that ζ is a fixed primitive p -th root of unity in $\overline{\mathbb{Q}}$, K is the cyclotomic field $\mathbb{Q}(\zeta)$ and $J_{p,r}$ is the Jacobian of the Hurwitz-Klein curve $F_{p,r}$ defined in the Introduction.

Koblitz and Rohrlich ([12]) showed that $J_{p,r}$ is isogenous to a cube of an absolutely simple abelian variety. Lim ([14]) explicitly computed the endomorphism ring of $J_{p,r}$ and proved that $J_{p,r}$ is K -isomorphic to a cube of an abelian variety. We now describe Lim's result:

For $i = 0, 1, 2$, let C_i denote the quotient curve of $F_{p,r}$ by the action of the automorphism group $\langle \zeta^{-i} \rho \zeta^i \rangle$. Let J_i be the Jacobian of C_i . Note that C_0 is defined over \mathbb{Q} and the curves C_i are all isomorphic over K . Lim showed that the natural projection maps

$$\phi_i : F_{p,r} \longrightarrow C_i$$

give rise, by Albanese functoriality, to a K -isogeny

$$\phi = \prod_{i=0}^2 \phi_i : J_{p,r} \longrightarrow \prod_{i=0}^2 J_i$$

whose kernel equals $J_{p,r}[\pi]$, where $\pi = \zeta - 1$. He then proceeded to show that there exists an isomorphism

$$f = \prod_{i=0}^2 f_i : J_{p,r} \longrightarrow \prod_{i=0}^2 J_i$$

defined over K such that $\phi_i = f_i \pi$, for $i = 0, 1, 2$.

For the specific case $p = 7$, this result was established by Prapavessi ([16]).

The fact that ϕ is only defined over K makes it difficult to compare the Mordell-Weil ranks of $J_{p,r}$ and J_0 over \mathbb{Q} . Identifying J_0 and $J_{p,r}$ with their duals, it follows immediately from the definition that the dual homomorphism

$$(\phi_0)^* : J_0 \longrightarrow J_{p,r}$$

satisfies the equalities

$$\begin{aligned} \phi_0 (\phi_0)^* &= 3, \\ (\phi_0)^* \phi_0 &= 1 + \rho + \rho^2. \end{aligned}$$

In particular, $(\phi_0)^*$ has finite kernel and the rank of $J_0(\mathbb{Q})$ equals the dimension of the kernel of the endomorphism $\rho - 1$ of the \mathbb{Q} -vector space $J_{p,r}(\mathbb{Q}) \otimes \mathbb{Q}$.

The following proposition shows in particular that the rank condition in Theorem 1.3 is equivalent to the following assertion:

$$\text{rk}(J_{p,r}(\mathbb{Q})) \stackrel{?}{=} \text{rk}(J_0(\mathbb{Q})).$$

Proposition 2.1. *Let M be any number field. Then*

$$\text{rk}(J_{p,r}(M)) \equiv \text{rk}(J_0(M)) \pmod{2}.$$

Proof of Proposition 2.1. We look at the isogeny decomposition of $J_{p,r}$ over \mathbb{Q} . Clearly, J_0 is a factor. Consider the abelian subvariety $B = (\rho - 1)J_{p,r}$ of $J_{p,r}$. It is easy to show that the map

$$J_{p,r} \xrightarrow{\phi_0 \times (\rho - 1)} J_0 \times B$$

is an isogeny defined over \mathbb{Q} . Hence, it suffices to show that $\text{rk}(B(M))$ is even. The automorphism ρ of $J_{p,r}$ induces an endomorphism θ of B such that $\theta^2 + \theta + 1 = 0$. Since the polynomial $X^2 + X + 1$ is irreducible over \mathbb{Q} , the elementary divisors of θ acting on the \mathbb{Q} -vector space $B(M) \otimes \mathbb{Q}$ are all equal to $X^2 + X + 1$. In particular, $B(M) \otimes \mathbb{Q}$ is a direct sum of two-dimensional cyclic θ -invariant subspaces, and this completes the proof.

Corollary 2.2. *If $\text{rk}(J_{p,r}(\mathbb{Q})) \leq 2$, then the Mordell-Weil rank condition in Theorem 1.3 is satisfied.*

Remark. It remains an open problem whether the inequality $\text{rk}(J_{p,r}(\mathbb{Q})) \leq 2$ holds in general. One possible approach is to perform a $(\zeta - 1)$ -descent on $J_{p,r}$ using its isogeny decomposition over K combined with results of Faddeev ([6]) and McCallum ([15]). For some time, the author was under the impression that the information on the corresponding Selmer and Shafarevich-Tate groups obtained by this approach produces examples where the inequality $\text{rk}(J_{p,r}(\mathbb{Q})) \leq 2$ fails. It turns out that this is not the case. At present, no counterexample to the latter inequality is known. We hope to address this question in joint work (in progress) with McCallum.

Proof of Corollary 2.2. By Proposition 2.1, we only need to show that we cannot have $\text{rk}(J_{p,r}(\mathbb{Q})) = 2$ and $\text{rk}(J_0(\mathbb{Q})) = 0$. If $p \geq 13$, this follows from the work of Gross and Rohrlich ([8]) together with the observation that the Gross-Rohrlich divisor class projects to a point of infinite order on J_0 (the Gross-Rohrlich divisor class is, up to torsion, ρ -invariant, therefore its image under $1 + \rho + \rho^2$ is also of infinite order). If $p = 7$, then both ranks are equal to 0 by a result of Faddeev ([6]). This proves the corollary.

We now want to take advantage of the fact that $J_{p,r}$ and J_0 have complex multiplication by $\mathbb{Z}[\zeta]$ and $\mathbb{Z}[\zeta + \zeta^r + \zeta^{r^2}]$, respectively (note that $\rho \zeta = \zeta^r \rho$, so the endomorphism $\zeta + \zeta^r + \zeta^{r^2}$ of $J_{p,r}$ commutes with ρ , hence induces an endomorphism of J_0). Let $L = \mathbb{Q}(\zeta + \zeta^r + \zeta^{r^2})$. Then $[K : L] = 3$. The following result is well known. We have not been able to find a reference, so we give a proof of it below.

Lemma 2.3. *We have the following equalities:*

- (a) $\text{rk}(J_{p,r}(K)) = (p - 1)\text{rk}(J_{p,r}(\mathbb{Q}))$.
- (b) $\text{rk}(J_{p,r}(L)) = (p - 1)\text{rk}(J_{p,r}(\mathbb{Q}))/3$.
- (c) $\text{rk}(J_0(L)) = (p - 1)\text{rk}(J_0(\mathbb{Q}))/3$.

Proof of Lemma 2.3. We only prove part (a). The proofs of the remaining parts are similar. Let $G = \text{Gal}(K/\mathbb{Q})$. Since ζ acts as complex multiplication on $J_{p,r}(K)$, the \mathbb{Q} -vector space $V = J_{p,r}(K) \otimes \mathbb{Q}$ has a K -vector space structure. With respect to this structure, the Galois action of G on V is semi-linear. Choosing a K -basis of V , we can thus interpret the action of G as an element of the Galois cohomology group $H^1(G, GL_n(K))$, where $n = \dim_K V$. By Hilbert’s Theorem 90, the latter group is trivial, therefore V is isomorphic to $V^G \otimes K$. In particular,

$$\text{rk}(J_{p,r}(K)) = \dim_{\mathbb{Q}} V = (\dim_{\mathbb{Q}} V^G)(\dim_{\mathbb{Q}} K) = (p - 1)\text{rk}(J_{p,r}(\mathbb{Q})).$$

Using Proposition 2.1, Lemma 2.3 and Lim’s results on the geometry of $J_{p,r}$ over K , one sees that the rank condition in Theorem 1.3 is reduced to any of the following equivalent assertions:

$$\begin{aligned} \text{rk}(\phi_0(J_{p,r}(L))) &\stackrel{?}{=} \text{rk}(J_{p,r}(L)), \\ \text{rk}(f_0((\zeta - 1)J_{p,r}(L))) &\stackrel{?}{=} \text{rk}(J_{p,r}(L)). \end{aligned}$$

We can only prove the following statement, which, nevertheless, will be used in the proof of Theorem 1.3:

Lemma 2.4. *We have:*

- (a) $\text{rk}(\phi_0(\zeta^k J_{p,r}(L))) = \text{rk}(J_{p,r}(L))$, for all $k \in \{1, \dots, p - 1\}$.
- (b) $\text{rk}(f_0((\zeta^k - 1)J_{p,r}(L))) = \text{rk}(J_{p,r}(L))$, for all $k \in \{2, 3, \dots, p - 1\}$.

Proof of Lemma 2.4. (a) Fix $k \in \{1, \dots, p - 1\}$. Suppose that the claim is false. Then there exists a point of infinite order $D \in J(L)$ such that $\phi_0(\zeta^k D) = 0$. Therefore $(1 + \rho + \rho^2)(\zeta^k D) = 0$. Consider the abelian group

$$G = \{\zeta^k D_1 + \zeta^{kr} D_2 + \zeta^{kr^2} D_3 : D_i \in J_{p,r}(L), i = 1, 2, 3\}.$$

Since $J_{p,r}$ is K -isomorphic to J_0^3 , we have $3\text{rk}(J_0(K)) = \text{rk}(J_{p,r}(K))$ and, by Lemma 2.3, $\text{rk}(\text{Ker}(\phi_0)) = 2\text{rk}(J_{p,r}(L))$. Note that, by the proof of Lemma 2.3, we have $G \otimes \mathbb{Q} = J_{p,r}(K) \otimes \mathbb{Q}$. Therefore, $\text{rk}(\text{Ker}(\phi_0) \cap G) = 2\text{rk}(J_{p,r}(L))$. Now consider the following subgroup H of G :

$$H = \{\zeta^k D_1 + \zeta^{kr} D_2 + \zeta^{kr^2} D_3 : D_1 + D_2^{\rho^2} + D_3^{\rho} = \lambda D, \lambda \in \mathbb{Z}\}.$$

H has rank strictly greater than $2\text{rk}(J_{p,r}(L))$, since we can choose D_2 and D_3 to be any points of infinite order in $J_{p,r}(L)$ and we still have infinitely many choices for D_1 . However, since $\rho \zeta = \zeta^r \rho$, it is trivial to check that, for $F \in H$, $(1 + \rho + \rho^2)(F) = (1 + \rho + \rho^2)(\lambda \zeta^k D) = 0$. Hence, $H \subseteq \text{Ker}(\phi_0) \cap G$, which is impossible by the above discussion regarding the ranks of these groups.

(b) Fix $k \in \{2, 3, \dots, p - 1\}$. Set

$$\eta_i = \sum_{j=0}^{k-1} \zeta^{jr^i},$$

for $i = 0, 1, 2$. Since $\phi_0 = f_0 \pi$, it suffices to show that there is no point D of infinite order in $J_{p,r}(L)$ such that $(1 + \rho + \rho^2)(\eta_0 D) = 0$. Suppose this were not the case. Applying $Gal(K/L)$ to the latter equality we get the system

$$\begin{aligned} \eta_0 D + \eta_1 D^\rho + \eta_2 D^{\rho^2} &= 0, \\ \eta_1 D + \eta_2 D^\rho + \eta_0 D^{\rho^2} &= 0, \\ \eta_2 D + \eta_0 D^\rho + \eta_1 D^{\rho^2} &= 0. \end{aligned}$$

Eliminating D^ρ and D^{ρ^2} from the above system, we get

$$((\eta_0^2 - \eta_1 \eta_2)^2 - (\eta_1^2 - \eta_0 \eta_2)(\eta_2^2 - \eta_0 \eta_1)) D = 0.$$

It is easy to check that the coefficient of D is a non-zero element in $\mathbb{Z}[\zeta]$. Multiplying the latter equality by an appropriate integer in $\mathbb{Z}[\zeta]$, we obtain $sD = 0$, for a non-zero integer $s \in \mathbb{Z}$ (we can take s to be the K/\mathbb{Q} -norm of the original coefficient). This implies that D is torsion, which is a contradiction.

3. ALGEBRAIC POINTS OF LOW DEGREE

In this section we will prove Theorem 1.3. Consider the cusps on (the first model of) $F_{p,r}$:

$$a = (0, 0), \quad b = (1, 0), \quad c = \infty.$$

Note that ρ induces a permutation of $\{a, b, \infty\}$ of order 3 and ζ fixes each of these three points. By the work of Gross and Rohrlich ([8]), the difference between any two cusps is a p -torsion point on $J_{p,r}$. For a point P_1 on $F_{p,r}$ of degree k over \mathbb{Q} , let P_1, \dots, P_k be the Galois conjugates of P_1 . Let D be the following point in $J_{p,r}(\mathbb{Q})$:

$$D = [P_1 + \dots + P_k - k\infty].$$

Lemma 3.1. *Let $p \geq 13$. Suppose that $P_1 \neq a, b, \infty$.*

- (a) *If $k \leq 2$, then D is of infinite order.*
- (b) *If $k = 3$ and the gonality γ of $F_{p,r}$ satisfies $\gamma \geq 4$, then D is of infinite order.*

Proof of Lemma 3.1. Suppose that D is torsion. By the work of Gross and Rohrlich ([8]), D has to be invariant under ζ . In other words, the divisor

$$P_1 + \dots + P_k - (\zeta P_1 + \dots + \zeta P_k)$$

is principal.

(a) By a result of Coleman ([3]), $F_{p,r}$ is not hyperelliptic, hence $\gamma \geq 3$. Therefore, since $k \leq 2$, the latter divisor is equal to 0. If $k = 1$, this amounts to $P_1 = \zeta P_1$, which is absurd, since the left-hand side is \mathbb{Q} -rational, while the right-hand side is not. Similarly, if $k = 2$, the only possibility is

$$P_1 = \zeta P_2, \quad P_2 = \zeta P_1.$$

But then $P_1 = \zeta^2 P_1$. Using the first model of $F_{p,r}$, this amounts to $(x, y) = (x, \zeta^2 y)$, so $y = 0$, hence P_1 is a cusp, which is a contradiction.

(b) By the gonality assumption, we have

$$\sum_{i=1}^3 P_i = \sum_{i=1}^3 \zeta P_i.$$

As in part (a), we cannot have $P_i = \zeta P_i$, for any i . Therefore, $P_1 = \zeta P_2$, $P_2 = \zeta P_3$ and $P_3 = \zeta P_1$ or $P_1 = \zeta P_3$, $P_2 = \zeta P_1$ and $P_3 = \zeta P_2$. In either of these cases, $P_1 = \zeta^3 P_1$, which is absurd, as in part (a).

Proof of Theorem 1.3 for $p \geq 13$. Assume that the Mordell-Weil rank condition in Theorem 1.3 is satisfied. By Proposition 2.1, we have $\text{rk}(J_0(\mathbb{Q})) = \text{rk}(J_{p,r}(\mathbb{Q}))$. By the discussion preceding Proposition 2.1, this means that $D^\rho - D$ is torsion, for every $D \in J_{p,r}(\mathbb{Q})$.

Now let P_1 be a point on $F_{p,r}$ of degree k over \mathbb{Q} (where $k=1$ or 2). Suppose that $P_1 \neq a, b, \infty$. Form the corresponding \mathbb{Q} -rational point D in $J_{p,r}(\mathbb{Q})$, as in Lemma 3.1. It follows from Lemma 3.1 that D is of infinite order. Also, by the preceding paragraph, $D^\rho - D$ is torsion. Since the difference between any two cusps is also torsion, we get that

$$[P_1 + \dots + P_k - P_1^\rho - \dots - P_k^\rho]$$

is torsion. We now distinguish two cases:

Case 1: Suppose that $p \geq 19$. By [8], the latter divisor class is invariant by ζ . In other words, there exists a rational function on $F_{p,r}$ whose divisor equals

$$P_1 + \dots + P_k + \zeta P_1^\rho + \dots + \zeta P_k^\rho - (P_1^\rho + \dots + P_k^\rho + \zeta P_1 + \dots + \zeta P_k).$$

If $k = 1$, then, since the gonality γ of $F_{p,r}$ satisfies $\gamma \geq 3$, we get that

$$P_1 + \zeta P_1^\rho = P_1^\rho + \zeta P_1.$$

We cannot have $P_1 = \zeta P_1$, because the left-hand side is defined over \mathbb{Q} , while the right-hand side is not. Hence, $P_1 = P_1^\rho$. In terms of coordinates (using the second model of $F_{p,r}$), this means $xy = 1$ and $x = y^2$. Hence, since $x, y \in \mathbb{Q}$, we get $x = y = 1$, which is impossible because $(1, 1)$ is not a point on $F_{p,r}$.

Now suppose that $k = 2$. Since $\phi_0(P_i) = \phi_0(P_i^\rho)$, we get that the divisor

$$\phi_0(\zeta P_1^\rho) + \phi_0(\zeta P_2^\rho) - \phi_0(\zeta P_1) - \phi_0(\zeta P_2)$$

on C_0 is principal. Let E be the divisor $\phi_0(\zeta P_1) + \phi_0(\zeta P_2)$. Since $p \geq 19$, the genus of C_0 (which equals $(p - 1)/6$) is at least 3. Hence, by Riemann-Roch (notation as in [1]), we get $l(E) \leq l(K - E)$, so E is a special divisor. By Clifford's theorem, $\dim|E| = 0$ unless C_0 is hyperelliptic and $|E|$ equals the unique g_2^1 on C_0 .

In the latter case, the points $\phi_0(\zeta P_1)$ and $\phi_0(\zeta P_2)$ are conjugate under the hyperelliptic involution of C_0 . Since the latter involution acts as multiplication by -1 on J_0 , we see that

$$[\phi_0(\zeta P_1) + \phi_0(\zeta P_2) - 2\phi_0(\infty)] = 0.$$

In other words, the divisor class $\zeta[P_1 + P_2 - 2\infty] \in \zeta J_{p,r}(\mathbb{Q})$ projects to 0 under ϕ_0 . By Lemma 2.4(a), this means that $[P_1 + P_2 - 2\infty]$ is torsion, which is impossible, by Lemma 3.1.

Therefore, we must have $\dim|E| = 0$. This implies that

$$\phi_0(\zeta P_1^\rho) + \phi_0(\zeta P_2^\rho) = \phi_0(\zeta P_1) + \phi_0(\zeta P_2).$$

If $\phi_0(\zeta P_1^\rho) = \phi_0(\zeta P_1)$, then we have the following possibilities:

(i) $\zeta P_1^\rho = \zeta P_1$. Then $P_1^\rho = P_1$, so, in terms of the second model of $F_{p,r}$, we have $xy = 1$ and $x = y^2$. This implies that $(x, y) = (\eta, \eta^2)$ or (η^2, η) , where η is a primitive cube root of unity in $\overline{\mathbb{Q}}$. So we have recovered the Gross-Rohrlich points ([8]).

(ii) $\zeta P_1^\rho = \zeta^r P_1^\rho$ or $\zeta^{r^2} P_1^{\rho^2}$. Then $P_1^\rho = \zeta^{r-1} P_1^\rho$ or $\zeta^{r^2-1} P_1^{\rho^2}$. This is impossible, since the left-hand side is defined over a quadratic field, while the right-hand side is not.

The only other option is $\phi_0(\zeta P_1^\rho) = \phi_0(\zeta P_2)$ and $\phi_0(\zeta P_2^\rho) = \phi_0(\zeta P_1)$. As above, for rationality reasons, we cannot have $\zeta P_1^\rho = \zeta^r P_2^\rho$ or $\zeta^{r^2} P_2^{\rho^2}$. Therefore, we must have $\zeta P_1^\rho = \zeta P_2$ and, similarly, $\zeta P_2^\rho = \zeta P_1$. Hence, $P_1^\rho = P_2$ and $P_2^\rho = P_1$. This shows that $P_1 = P_1^{\rho^2}$ and, as before, P_1 is a Gross-Rohrlich point. But then $P_1^\rho = P_1 \neq P_2$, a contradiction.

Case 2: Suppose that $p = 13$. Note that the curve $F_{13,3}$ has the smooth plane model $x^4y + y^4 + x = 0$. Therefore, $\gamma = 4$. The proof of Case 1 above goes through for $k = 1$. For $k = 2$, part of the proof goes through, up to the point where we show that there exists a rational function on $F_{p,r}$ whose divisor equals

$$P_1 + P_2 + \zeta P_1^\rho + \zeta P_2^\rho - P_1^\rho - P_2^\rho - \zeta P_1 - \zeta P_2.$$

Let $E = P_1^\rho + P_2^\rho + \zeta P_1 + \zeta P_2$. By Riemann-Roch, E is special. By Clifford's theorem, $\dim|E| \leq 1$, since E is not the canonical divisor (by degree) and $F_{13,3}$ is non-hyperelliptic.

Suppose $\dim|E| = 0$. Then

$$P_1 + P_2 + \zeta P_1^\rho + \zeta P_2^\rho = P_1^\rho + P_2^\rho + \zeta P_1 + \zeta P_2.$$

For rationality reasons, none of P_1^ρ or P_2^ρ can equal one of ζP_1^ρ or ζP_2^ρ . Therefore, we must have $P_1^\rho + P_2^\rho = P_1 + P_2$. If $P_1^\rho = P_1$, then, as before, we recover the Gross-Rohrlich points. If $P_1^\rho = P_2$, then also $P_2^\rho = P_1$, so $P_1 = P_1^{\rho^2}$, and, as before, this is a contradiction.

Otherwise, if $\dim|E| = 1$, then, by a well-known theorem in the geometry of smooth plane curves (see [1], exercise 18, page 56), there exists a line L in \mathbb{P}^2 such that

$$E = L.F_{13,3} - P,$$

where P is a point on $F_{13,3}$.

Using the fact that $[P_1 + P_2 - P_1^\rho - P_2^\rho]$ is also invariant under ζ^2 and arguing exactly as above, we get that for the divisor $E' = P_1^\rho + P_2^\rho + \zeta^2 P_1 + \zeta^2 P_2$ there exists a line L' in \mathbb{P}^2 such that

$$E' = L'.F_{13,3} - Q,$$

where Q is a point on $F_{13,3}$ (if $\dim|E'| = 0$, we are done by the previous analysis).

But then L and L' have the points P_1^ρ and P_2^ρ in common, so they must coincide. Therefore, one of the points $\zeta^2 P_1$ or $\zeta^2 P_2$ has to equal one of the points ζP_1 or ζP_2 . As before, this is impossible for rationality reasons.

Proof of Theorem 1.3 for $p = 7$. Our curve $F_{7,2}$ is the Klein curve $x^3y + y^3 + x = 0$. It is a smooth plane quartic, hence has gonality 3. We will temporarily use the model $y^7 = x(1-x)^2$ of $F_{7,2}$. Let us first recall that, by a result of Faddeev ([6]), $J_{7,2}(\mathbb{Q})$ is finite. Also, let P and \overline{P} be the two quadratic points on $F_{7,2}$ that Gross

and Rohrllich described. In fact, it follows from [8] that 2 divides the order of $[P + \overline{P} - 2\infty]$. Therefore, by [8], any \mathbb{Q} -rational point on $J_{7,2}$ can be expressed as a \mathbb{Z} -linear combination of $[3P + 3\overline{P} - 2a - 2b - 2\infty]$ and $[a - b]$. Since the first divisor class is invariant under ρ , it follows that for $D \in J_{7,2}(\mathbb{Q})$, we have $D^\rho - D \in J_{7,2}$ [7]. Following the notation in [8], we conclude that, in particular,

$$[P_1 + \dots + P_k - P_1^\rho - \dots - P_k^\rho] = l[D_1 - D_\infty],$$

where $0 \leq l \leq 6$, $D_1 = a - b$ and $D_\infty = a - \infty$. From the given model of $F_{7,2}$ and the discussion in [8] (pages 203-204), it follows that

$$3[D_\infty] = 2[D_1].$$

Using the latter equality, we get the following cases:

- If $l = 6$, then $P_1 + \dots + P_k - P_1^\rho - \dots - P_k^\rho \sim 6D_1 - 6D_\infty \sim D_\infty - D_1 = b - \infty$.
- If $l = 5$, then $P_1 + \dots + P_k - P_1^\rho - \dots - P_k^\rho \sim 2D_\infty - 2D_1 \sim -D_\infty = \infty - a$.
- If $l = 4$, then $P_1 + \dots + P_k - P_1^\rho - \dots - P_k^\rho \sim 3D_\infty - 3D_1 = -D_1 = b - a$.
- If $l = 3$, then $P_1 + \dots + P_k - P_1^\rho - \dots - P_k^\rho \sim 3D_1 - 3D_\infty = D_1 = a - b$.
- If $l = 2$, then $P_1 + \dots + P_k - P_1^\rho - \dots - P_k^\rho \sim 2D_1 - 2D_\infty = D_\infty = a - \infty$.
- If $l = 1$, then $P_1 + \dots + P_k - P_1^\rho - \dots - P_k^\rho \sim D_1 - D_\infty \sim \infty - b$.
- If $l = 0$, then $P_1 + \dots + P_k - P_1^\rho - \dots - P_k^\rho \sim 0$.

Now, if $k = 1$, the above equivalences are equalities, because the gonality of $F_{7,2}$ equals 3. Since P_1 is not a cusp, we reach a contradiction.

Otherwise, suppose $k = 2$. We now use the smooth plane model of $F_{7,2}$. In all of the above cases, we can write

$$P_1 + P_2 + Q \sim P_1^\rho + P_2^\rho + R,$$

where R and Q are cusps. Let $E = P_1 + P_2 + Q$. By Riemann-Roch and Clifford's theorem, either $\dim|E| = 0$ or E is special and $\dim|E| = 1$.

In the former case, we get

$$P_1 + P_2 + Q = P_1^\rho + P_2^\rho + R.$$

Since P_1 is not \mathbb{Q} -rational, we necessarily have $Q = R$, so $P_1 + P_2 = P_1^\rho + P_2^\rho$, so, as before, we recover the Gross-Rohrllich points.

In the latter case, we can argue again by means of exercise 18, page 56 in [1]. We can find a line L in \mathbb{P}^2 and a point Q' on $F_{7,2}$ such that

$$P_1 + P_2 + Q + Q' = L.F_{7,2}.$$

Since two points determine a line and the divisor $P_1 + P_2 + Q$ is \mathbb{Q} -rational, we conclude that $L = L^\sigma$ for all $\sigma \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, so L is a \mathbb{Q} -rational line, hence Q' is also a \mathbb{Q} -rational point.

Now if $Q = Q'$, then L is the tangent line to $F_{7,2}$ at Q , so an easy calculation shows that P_1 and P_2 are cusps, which is impossible since P_1 is not \mathbb{Q} -rational. Therefore, $Q \neq Q'$, in which case L connects two cusps. Therefore, both P_1 and P_2 have to be cusps, a contradiction.

This completes the proof of Theorem 1.3. Note that since $F_{p,r}$ is covered by F_p by means of an explicit map (see [8]), the results automatically transfer to F_p (a point of degree $\leq k$ on F_p necessarily projects to a point of degree $\leq k$ on $F_{p,r}$ and knowing the latter determines the former).

Remark. The rank condition in Theorem 1.3 is satisfied for $p = 7$, since Faddeev showed in [6] that $\text{rk}(J_{7,2}(\mathbb{Q})) = 0$. The rank condition is also satisfied for $p = 13$.

In that case, we know that $\text{rk}(J_{13,3}(\mathbb{Q})) = 1$, by the work of Faddeev and Gross-Rohrlich (see [8], second table on page 219). Therefore, by Theorem 1.3, we know all the points of degree ≤ 2 on $F_{7,2}$ and $F_{13,3}$. We now describe how similar results can be obtained for the Hurwitz-Klein curves mentioned in the Introduction. For an integer $m \geq 3$, the curves

$$H_m : x^m y + y^m + x = 0, \quad G_m : y^{m^2-m+1} = x(1-x)^{m-1}$$

are birationally isomorphic by means of the maps

$$\begin{aligned} H_m &\longrightarrow G_m, & G_m &\longrightarrow H_m, \\ (x, y) &\mapsto \left(\frac{-x}{y^m}, \frac{(-1)^m x}{y}\right), & (a, b) &\mapsto \left(\frac{a-1}{b^{m-1}}, \frac{(-1)^m (a-1)}{b^m}\right), \end{aligned}$$

respectively.

(i) Suppose m is of the form $7s + 3$ or $7s + 5$, with $s \in \mathbb{Z}$. Then $m^2 - m + 1 = 7t$ for some integer t . Consider the maps $G_m \rightarrow G_3$ and $G_m \rightarrow G'_3$ given by

$$(x, y) \mapsto \left(x, \frac{y^t}{(1-x)^s}\right),$$

where G'_3 is the curve $y^7 = x(1-x)^4$. Since we know all the points of degree ≤ 2 on $F_{7,2}$ and G_3 , G'_3 are isomorphic to $F_{7,2}$ (see [3]), the only possible quadratic points on H_m are the Gross-Rohrlich points which lie on H_m if and only if 3 does not divide $m - 2$.

(ii) Suppose m is of the form $13s + 4$ or $13s + 10$, with $s \in \mathbb{Z}$. Then $m^2 - m + 1 = 13t$ for some integer t . Consider the maps $G_m \rightarrow G_4$ and $G_m \rightarrow G'_4$ given by

$$(x, y) \mapsto \left(x, \frac{y^t}{(1-x)^s}\right),$$

where G'_4 is the curve $y^{13} = x(1-x)^9$. As in the previous case, since we know all the points of degree ≤ 2 on $F_{13,3}$ and G_4 and G'_4 are isomorphic to $F_{13,3}$ (see [3]), the only possible quadratic points on H_m are the Gross-Rohrlich points which lie on H_m if and only if 3 does not divide $m - 2$.

4. PROOF OF THE MAIN RESULT

The statement about points of degree ≤ 2 on F_{13} follows from Theorem 1.3, since the hypothesis of Corollary 2.2 is satisfied in this case by the results of Faddeev (see [6], paragraph 8, page 68). We will first describe all points of degree 3 on the curve $F_{13,3}$. Let P_1 be such a point. We will argue as in the proof of Theorem 1.3 for $p = 7$. We use the model $y^{13} = x(1-x)^3$ of $F_{13,3}$. As in the latter proof, we have that

$$[P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho] = l[D_1 - D_\infty],$$

where $0 \leq l \leq 12$, $D_1 = a - b$ and $D_\infty = a - \infty$. By [8], we have

$$4[D_\infty] = 3[D_1].$$

We have the following cases:

- If $l = 12$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim D_\infty - D_1 = b - \infty$.
- If $l = 11$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim 2D_\infty - 2D_1 = 2b - 2\infty$.
- If $l = 10$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim 3D_\infty - 3D_1 = -D_\infty = \infty - a$.
- If $l = 9$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim -D_1 = b - a$.
- If $l = 8$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim D_\infty - 2D_1 = 2b - a - \infty$.

- If $l = 7$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim -2D_\infty = 2\infty - 2a$.
- If $l = 6$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim 2D_\infty = 2a - 2\infty$.
- If $l = 5$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim 2D_1 - D_\infty = a + \infty - 2b$.
- If $l = 4$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim D_1 = a - b$.
- If $l = 3$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim D_\infty = a - \infty$.
- If $l = 2$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim 2D_1 - 2D_\infty = 2\infty - 2b$.
- If $l = 1$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim D_1 - D_\infty = \infty - b$.
- If $l = 0$, then $P_1 + P_2 + P_3 - P_1^\rho - P_2^\rho - P_3^\rho \sim 0$.

In the last case ($l = 0$), the equivalence must be an equality because the gonality of $F_{13,3}$ equals 4. We cannot have $P_1 = P_1^\rho$ because then, as before, P_1 would be one of the Gross-Rohrlich points. Hence, the Galois conjugates of P_1 are given by the action of $\langle \rho \rangle$ on P_1 .

In each of the remaining 12 cases ($l \neq 0$), we can add (if necessary) a cusp to both sides of the equivalence to get

$$P_1 + P_2 + P_3 + 2R \sim P_1^\rho + P_2^\rho + P_3^\rho + R' + R'',$$

where R, R' and R'' are cusps. Now let $E = P_1 + P_2 + P_3 + 2R$. By Riemann-Roch, $l(E) = l(K - E)$, so E is special. By Clifford's theorem, $\dim|E| \leq 2$.

If $\dim|E| = 0$, we conclude, as above, that the Galois conjugates of P_1 are given by the action of $\langle \rho \rangle$ on P_1 .

If $\dim|E| = 2$, then, by [1], $|E|$ is the unique g_5^2 on $F_{13,3}$ and is cut out by lines in \mathbb{P}^2 (recall that $F_{13,3}$ is a smooth plane quintic). In particular, there exists a line L in \mathbb{P}^2 such that $E = L.F_{13,3}$. If $\dim|E| = 1$, then, by a result of Coppens ([4]), there exists a line L in \mathbb{P}^2 such that $E = L.F_{13,3}$. In both cases, the line L is therefore the tangent line to $F_{13,3}$ at R . Since R is a cusp, we conclude that P_1, P_2 and P_3 are also cusps, which is impossible.

We have thus proved that the Galois orbit of a cubic point on $F_{13,3}$ is contained in its $\langle \rho \rangle$ -orbit. It turns out that we get cubic points on $F_{13,3}$ by intersecting the smooth plane model of the curve with the line $x + y + 1 = 0$ or with the conic $xy + x + y = 0$. Hence there are at least 6 cubic points on $F_{13,3}$. We now want to give an upper bound for the number of such points. This can be done as follows:

Let P_1 be a cubic point on $F_{13,3}$. Consider the projection map

$$F_{13,3} \xrightarrow{\phi_0} C_0.$$

Since Galois conjugation acts by $\langle \rho \rangle$ on P_1 , it is immediate that $\phi_0(P_1)$ is \mathbb{Q} -rational. Since C_0 has genus 2 and Mordell-Weil rank 1 over \mathbb{Q} , we can apply Coleman's effective Chabauty ([2]): C_0 has good reduction at 3, therefore, by [2], Corollary 4b(i), we get $\#C(\mathbb{Q}) \leq 12$. One of the \mathbb{Q} -rational points on C_0 is the projection of a cusp on $F_{13,3}$, so it must be discarded. Therefore there are at most 11 remaining \mathbb{Q} -rational points and they can be obtained by at most 33 cubic points on $F_{13,3}$, and this is our upper bound.

Now let us see how to transfer the above information to cubic points on F_{13} . First note that the map

$$F_{13} \xrightarrow{g} F_{13,3}$$

given by

$$(x, y) \mapsto (-x^{13}, x^3y)$$

(using the first model of $F_{13,3}$) is injective on cubic points, because if for two cubic points (a, b) and (c, d) on F_{13} we have $g(a, b) = g(c, d)$, then $a/c = \zeta^l$ for some l .

If 13 does not divide l , we have a contradiction, since the field of definition of a/c cannot exceed 9. Therefore, $a = c$, so $b = d$ also.

Also the six known cubic points on $F_{13,3}$ (obtained by intersecting the smooth plane model of $F_{13,3}$ with the line $x + y + 1 = 0$ or with the conic $xy + x + y = 0$) do not lift to cubic points on F_{13} . Hence there are at most 27 cubic points on F_{13} . The assertion about their Galois orbits is established as follows:

Let $P_1 = (x, y)$ be a cubic point on F_{13} . Consider the automorphism (also denoted by ρ) of F_{13} given by $\rho(x, y) = (1/y, x/y)$. By what we saw above we have

$$g(P_1) + g(P_2) + g(P_3) = g(P_1)^\rho + g(P_1)^\rho + g(P_1)^\rho.$$

Let σ and τ be the non-trivial embeddings of the field of definition of P_1 in $\overline{\mathbb{Q}}$. Using the first model of $F_{13,3}$, the automorphism ρ is given by

$$(x, y) \mapsto (1/(1-x), -x/y^4).$$

Therefore,

$$\begin{aligned} &(-x^{13}, x^3y) + (-(x^\sigma)^{13}, (x^\sigma)^3y^\sigma) + (-(x^\tau)^{13}, (x^\tau)^3y^\tau) \\ &= (-x^{13}, x^3y) + (-1/y^{13}, x/y^4) + (-y^{13}/x^{13}, y^3/x^4). \end{aligned}$$

Without loss of generality, we may assume that the second summands of the left- and right-hand side are equal. Then $(x^\sigma y)^{13} = 1$ and $(x^\sigma)^3 y^4 y^\sigma = x$. But $x^\sigma y$ lies in the Galois closure of the field of definition of P_1 , hence has degree at most 6 over \mathbb{Q} . Therefore, we get $x^\sigma y = 1$ and $yy^\sigma = x$. In other words,

$$(x^\sigma, y^\sigma) = (1/y, x/y) = \rho(x, y),$$

and the assertion is proved.

ACKNOWLEDGMENTS

I am grateful to William McCallum for sharing with me his insights on the subject via numerous conversations. I thank Robert Coleman, Minhyong Kim, Fernando Rodriguez Villegas and David Rohrlich for their remarks. The constructive criticism of an anonymous referee regarding the exposition is also greatly appreciated.

REFERENCES

- [1] E. Arbarello, M. Cornalba, P. Griffiths and J. Harris: *Geometry of algebraic curves I*, Grundlehren der Math. Wiss. **247**, Springer-Verlag, New York, 1985. MR **86h**:14019
- [2] R. Coleman: *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765-770. MR **87f**:11043
- [3] R. Coleman: *Torsion points on abelian étale coverings of $\mathbb{P}^1 - \{0, 1, \infty\}$* , Trans. Amer. Math. Soc. **311** (1989), no. 1, 185-208. MR **90a**:11064
- [4] M. Coppens: *A study of the schemes W_e^1 of smooth plane curves*, in Proc. 1st Belgian-Spanish Week on Algebra and Geometry, R.U.C.A (1988), 29-63.
- [5] O. Debarre and M. Klassen: *Points of low degree on smooth plane curves*, J. Reine Angew. Math. **446** (1994), 81-87. MR **95f**:14052
- [6] D. Faddeev: *On the divisor class groups of some algebraic curves*, Soviet Math. Dokl. **2** (1961), 67-69. MR **24**:A723
- [7] G. Faltings: *Diophantine approximation on abelian varieties*, Ann. Math. **133** (1991), 549-576. MR **93d**:11066
- [8] 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. MR **58**:10911
- [9] A. Hurwitz: *Über die diophantische Gleichung $x^3y + y^3 + x = 0$* , Math. Ann. **65** (1908), 428-430.
- [10] M. Klassen and P. Tzermias: *Algebraic points of low degree on the Fermat quintic*, Acta Arith. **82** (1997), no. 4, 393-401. MR **98k**:11086

- [11] F. Klein: *Über die Transformation siebenter Ordnung der elliptischen Funktionen*, Gesammelte Math. Abhandlungen III **84**, Springer, Berlin, 1923.
- [12] N. Koblitz and D. Rohrlich: *Simple factors in the Jacobian of a Fermat curve*, Canadian J. Math., **30** (1978), no. 6, 1183-1205. MR **80d**:14022
- [13] S. Lefschetz: *A Class of Algebraic Curves with Cyclic Group and their Jacobian Varieties*, 163-178, in *Selected Papers*, Chelsea, New York, 1971. MR **45**:8495
- [14] C.-H. Lim: *The Jacobian of a cyclic quotient of a Fermat curve*, Nagoya Math. J. **125** (1992), 73-92. MR **93i**:14024
- [15] W. McCallum: *On the Shafarevich-Tate group of the Jacobian of a quotient of the Fermat curve*, Invent. Math. **93** (1988), no. 3, 637-666. MR **90b**:11059
- [16] D. Prapavessi: *On the Jacobian of the Klein curve*, Proc. Amer. Math. Soc. **122** (1994), no. 4, 971-978. MR **95b**:14023
- [17] P. Ribenboim: *Homework!*, Proc. 5th Conf. Canad. Number Th. Assoc., Ottawa (1996), 391-392, Amer. Math. Soc., Providence (1999).
- [18] R. Taylor and A. Wiles: *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995), no. 3, 553-572. MR **96d**:11072
- [19] P. Tzermias: *Algebraic points of low degree on the Fermat curve of degree seven*, Manuscripta Math. **97** (1998), 483-488. MR **99j**:11075
- [20] P. Tzermias: *Parametrization of low-degree points on a Fermat curve*, submitted for publication.
- [21] A. Wiles: *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), no. 3, 443-551. MR **96d**:11071

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF TENNESSEE, KNOXVILLE, TENNESSEE 37996-1300

E-mail address: `tzermias@math.utk.edu`