ACTA ARITHMETICA
117.3 (2005)

Improved bounds on the number of low-degree points on certain curves

by

PAVLOS TZERMIAS (Knoxville, TN)

1. Introduction. Let $\mathbb{Q}$ be the field of rational numbers and $\overline{\mathbb{Q}}$ a fixed algebraic closure of $\mathbb{Q}$. If C is a smooth projective curve defined over $\mathbb{Q}$, a point $P \in C(\overline{\mathbb{Q}})$ is said to be of *degree* k over $\mathbb{Q}$ if its field of definition is an extension of $\mathbb{Q}$ of degree k. If C is a smooth plane curve of gonality γ (i.e., γ is the smallest degree of a morphism from C to $\mathbb{P}^1$), a point on C of degree at most $\gamma - 1$ over $\mathbb{Q}$ is called a *low-degree point* on C. Under certain (and quite general) conditions, the set of low-degree points on such a curve C is finite, as proven by Debarre and Klassen ([DK]) using results of Faltings ([F]). In what follows, we exclude any discussion of the case $k = 1$ (i.e. the case of $\mathbb{Q}$-rational points). For some Fermat curves of prime degree $p \geq 5$, explicit (full or partial) results describing the low-degree points have appeared in the literature (see [GR], [KT], [T1], [T2], [T3], [MT]). For results regarding higher-degree points on certain Fermat curves, we refer the reader to [S]. Recall that the *Fermat curve* F_p of degree p is given by the equation $X^p + Y^p + Z^p = 0$. We also denote by H_5 the *Hurwitz–Klein curve* given by the equation $X^4Y + Y^4Z + Z^4X = 0$; the curve H_5 is also known as the *Snyder quintic*. As explained in [T3], H_5 is a quotient of F_{13}.

The purpose of this paper is to improve the bounds obtained in [T2] and [T3] on the number of points of degree 6 on F_{11}, the number of points of degree 3 on H_5 and the number of points of degree 3 on F_{13}. Note that by [GR], [T3], all points on these curves of degree lower than the one indicated above have been explicitly determined; in each case, there are only two such points and they are quadratic over $\mathbb{Q}$. Our main tool will be the remarkable improvement of Coleman's effective Chabauty bound ([C]) given by Lorenzini and Tucker in [LT].

Identify the symmetric group S_3 with the group of automorphisms of the Fermat curve obtained by permuting the letters X, Y and Z. Also denote by ϱ the 3-cycle in S_3 defined by $\varrho(X, Y, Z) = (Y, Z, X)$. Then ϱ (viewed

2000 *Mathematics Subject Classification*: Primary 11G30, 14H25.

both as an automorphism of F_{13} and of H_5) commutes with the morphism $F_{13} \to H_5$ described in [T3]. The following two results improve Theorem 1.2 in [T2] and Theorem 1.2 in [T3], respectively:

THEOREM 1.1. *There exist at most* 84 *points of degree* 6 *on* F_{11} *and the Galois orbit of each of these points equals its* S_3*-orbit.*

THEOREM 1.2. *There exist at most* 21 *cubic points on* H_5 *and at most* 15 *cubic points on* F_{13}*. The Galois orbit of each of these points equals its* $\langle \varrho \rangle$*-orbit.*

The statements about the Galois orbits have already been proven in [T2] and [T3], so it remains to establish the stated bounds in the above theorems. For the reader's convenience, we recall that the bounds obtained in [T2] and [T3] gave at most 120 (resp. 33, 27) such points on F_{11} (resp. H_5, F_{13}).

2. Proof of Theorem 1.1. Let C be a smooth projective model of the curve obtained as the quotient of F_{11} by the action of S_3. Both C and the projection map $\phi : F_{11} \to C$ are defined over $\mathbb{Q}$. In [T2] we showed that C has genus 5, its Jacobian has Mordell–Weil rank 1 over $\mathbb{Q}$ and the Galois orbits of points of degree at most 6 on F_{11} are in bijective correspondence with the $\mathbb{Q}$-rational points on the curve C. Moreover, an affine model for C is given by

$$\begin{aligned}\mathcal{E}:\ & r^{11}+22r^{10}-11r^9s+121r^9-187r^8s+44r^7s^2-374r^8-616r^7s+528r^6s^2\\ & -77r^5s^3-4004r^7+3432r^6s+605r^5s^2-550r^4s^3+55r^3s^4+1672r^6\\ & +13332r^5s-7590r^4s^2+440r^3s^3+154r^2s^4-11rs^5+39523r^5\\ & -30481r^4s-3905r^3s^2+3597r^2s^3-319rs^4-30250r^4-45331r^3s\\ & +31064r^2s^2-3652rs^3-108009r^3+117557r^2s-20625rs^2\\ & +164450r^2-57453rs-63151r-1=0.\end{aligned}$$

We will now use the Lorenzini–Tucker result ([LT]) to give a new upper bound on the number of $\mathbb{Q}$-rational points on C. The argument is very similar to the one given in [T2], but we include it here for the sake of completeness. Note that F_{11} has good reduction at $p = 5$, hence so does C. Let $\widetilde{C}$ denote a smooth projective model of the reduction of C at $p = 5$. Applying Theorem 1.1 of [LT] (where $p = 5$ and $d = 2$) gives

$$\#C(\mathbb{Q}) \le \#\widetilde{C}(\mathbb{F}_5) + 10.$$

We first show that there are exactly 6 $\mathbb{F}_5$-rational points on $\widetilde{C}$. Let $\widetilde{F}_{11}$ be the reduction of F_{11} at $p = 5$. Also let $\widetilde{\mathcal{E}}$ denote the projectivization of the singular model of $\widetilde{C}$ obtained by reducing $\mathcal{E}$ at $p = 5$. We have morphisms of curves

$$\widetilde{F}_{11} \xrightarrow{\widetilde{\phi}} \widetilde{C} \xrightarrow{\widetilde{\pi}} \widetilde{\mathcal{E}},$$

where $\widetilde{\pi}$ is the normalization map and $\widetilde{\phi}$ is the reduction of ϕ at $p = 5$. Clearly, any $\mathbb{F}_5$-rational point on $\widetilde{C}$ maps to an $\mathbb{F}_5$-rational point on $\widetilde{\mathcal{E}}$ under $\widetilde{\pi}$. It is straightforward to check that $\widetilde{\mathcal{E}}$ has exactly 6 points defined over $\mathbb{F}_5$, namely the points (r, s) with coordinates $(1, 0)$, $(1, 1)$, $(1, 2)$, $(2, 1)$, $(3, 4)$ and the unique point at infinity. Now each of the five affine points listed above is a nonsingular point of $\widetilde{\mathcal{E}}$, so its fiber under $\widetilde{\pi}$ consists of a unique $\mathbb{F}_5$-rational point on $\widetilde{C}$. The point at infinity on $\widetilde{\mathcal{E}}$ is singular. We claim that, among the points in its fiber under $\widetilde{\pi}$, there is exactly one which is defined over $\mathbb{F}_5$.

To see this, note that any such point P lifts under $\widetilde{\phi}$ to a point at infinity R (i.e. one of the projective coordinates of R vanishes). Since P is $\mathbb{F}_5$-rational, every Galois conjugate of R belongs to the fiber $\widetilde{\phi}^{-1}(P)$, which in turn consists of the S_3-conjugates of R. If R is not defined over $\mathbb{F}_5$, then it is of degree 5 over $\mathbb{F}_5$, because the cyclotomic polynomial of degree 10 splits into a product of two irreducible factors of degree 5 over $\mathbb{F}_5$. Since there can be at most two S_3-conjugates of R with the same coordinate vanishing, we have a contradiction. It follows that R has to be equal to $(0, -1, 1)$, $(-1, 0, 1)$ or $(-1, 1, 0)$, and this proves that there exists exactly one such point P.

Therefore, there are exactly 6 $\mathbb{F}_5$-rational points on $\widetilde{C}$. This implies that there are at most $6 + 10 = 16$ $\mathbb{Q}$-rational points on C. Now the three $\mathbb{Q}$-rational and the two quadratic points on F_{11} project to two distinct $\mathbb{Q}$-rational points on C under the morphism ϕ. Therefore, there are at most 14 $\mathbb{Q}$-rational points on C which lift to points of degree 6 on F_{11}. Therefore, there are at most $14 \cdot 6 = 84$ points of degree 6 on F_{11}. This completes the proof of Theorem 1.1.

It should be noted that there are at least 6 known points of degree 6 on F_{11}; these points are obtained by intersecting F_{11} with the line $X + Y + Z = 0$ in $\mathbb{P}^2$. An easy calculation shows that these points are of the form $(c, -1 - c, 1)$, where c is a root of the equation

$$X^6 + 3X^5 + 7X^4 + 9X^3 + 7X^2 + 3X + 1 = 0.$$

Note also that the action of S_3 on F_{11} permutes the above points.

3. Proof of Theorem 1.2. Let X denote a smooth projective model of the curve obtained as the quotient of H_5 by the action of $\langle \varrho \rangle$. Both X and the natural projection map $\Phi :\ H_5 \to X$ of degree 3 are defined over $\mathbb{Q}$. The genus of X equals 2. As shown in [T3], the Jacobian of X has Mordell–Weil rank 1 over $\mathbb{Q}$ and the Galois orbits of points of degree 1 or 3 on H_5 are in bijective correspondence with the $\mathbb{Q}$-rational points on X. Note that the two quadratic points on H_5 are fixed by ϱ, so their images under Φ are not $\mathbb{Q}$-rational.

We now produce an explicit model for X:

PROPOSITION 3.1. *An affine model for X is given by*

$$\mathcal{X}:\ r^4 - 4sr^2 - 3sr + 4r + s^3 + 2s^2 + s + 3 = 0.$$

Proof. Let $h(r,s)$ be the left-hand side of the above equation. Consider the rational map

$$\ominus:\ \mathbb{C}^2 \to \mathbb{C}^2$$

given by $(x,y) \mapsto (r,s)$, where

$$r = x + \frac{1}{y} + \frac{y}{x}, \qquad s = y + \frac{1}{x} + \frac{x}{y}.$$

Let $\mathcal{H}_5$ be the affine curve $x^4y + y^4 + x = 0$. It suffices to show that $\ominus$ induces, by restriction, a rational map $\psi:\ \mathcal{H}_5 \to \mathcal{X}$ whose fiber above (r,s) equals

$$\left\{(x,y), \left(\frac{1}{y}, \frac{x}{y}\right), \left(\frac{y}{x}, \frac{1}{x}\right)\right\}$$

for all but finitely many $(r,s) \in \mathcal{X}(\mathbb{C})$. First we compute the fibers of $\ominus$. Fix $(r,s) \in \mathbb{C}^2$ and $(x,y) \in \ominus^{-1}(r,s)$. We claim that

$$\ominus^{-1}(r,s) = \left\{(x,y), \left(\frac{1}{y}, \frac{x}{y}\right), \left(\frac{y}{x}, \frac{1}{x}\right), \left(\frac{1}{y}, \frac{1}{x}\right), \left(\frac{y}{x}, y\right), \left(x, \frac{x}{y}\right)\right\}.$$

It is clear that all of the above six points are in $\ominus^{-1}(r,s)$. Now note that for any $(c,d) \in \ominus^{-1}(r,s)$, we have

$$d^3 - sd^2 + rd - 1 = 0, \qquad dc^2 + (1 - rd)c + d^2 = 0.$$

Therefore, there are at most six possible values for the pair (c,d) and this proves the claim. Now a straightforward calculation shows that

$$h(\ominus(x,y)) = \frac{(x^4y + y^4 + x)(x^4y^3 + y^4 + x^3)}{x^4y^4}.$$

In particular, ψ is a rational map from $\mathcal{H}_5$ to $\mathcal{X}$ and for $(r,s) \in \mathcal{X}(\mathbb{C})$ it follows that, for each $(x,y) \in \ominus^{-1}(r,s)$, either (x,y) or $(1/y, 1/x)$ is on $\mathcal{H}_5$. Note that, with the exception of finitely many cases, only one of the latter two points can lie on $\mathcal{H}_5$. By the above calculation of the fibers of $\ominus$ and the evident symmetry of ψ, the assertion follows. ■

Now we are ready to prove Theorem 1.2. Note that F_{13} has good reduction at $p = 5$, hence so do H_5 and X. Let $\widetilde{X}$ denote a smooth projective model of the reduction of X at $p = 5$. Applying Theorem 1.1 of [LT] (where $p = 5$ and $d = 1$) gives

$$\#X(\mathbb{Q}) \le \#\widetilde{X}(\mathbb{F}_5) + 2.$$

We first show that there are exactly 6 $\mathbb{F}_5$-rational points on $\widetilde{X}$. Let $\widetilde{H}_5$ be the reduction of H_5 at $p = 5$. Also let $\widetilde{\mathcal{X}}$ denote the projectivization of the singular model of $\widetilde{X}$ obtained by reducing $\mathcal{X}$ at $p = 5$. We have morphisms of curves

$$\widetilde{H}_5 \xrightarrow{\widetilde{\Phi}} \widetilde{X} \xrightarrow{\widetilde{\Pi}} \widetilde{\mathcal{X}},$$

where $\widetilde{\Pi}$ is the normalization map and $\widetilde{\Phi}$ is the reduction of Φ at $p = 5$. Clearly, any $\mathbb{F}_5$-rational point on $\widetilde{X}$ maps to an $\mathbb{F}_5$-rational point on $\widetilde{\mathcal{X}}$ under $\widetilde{\Pi}$. It is straighforward to check that $\widetilde{\mathcal{X}}$ has exactly 7 points defined over $\mathbb{F}_5$, namely the points (r, s) with coordinates $(1, 1)$, $(1, 3)$, $(1, 4)$, $(3, 1)$, $(4, 3)$, $(4, 0)$, and the unique point at infinity. Now the point at infinity and each of the first five affine points listed above is a nonsingular point on $\widetilde{\mathcal{X}}$, so its fiber under $\widetilde{\Pi}$ consists of a unique $\mathbb{F}_5$-rational point on $\widetilde{X}$. The point $(4, 0)$ on $\widetilde{\mathcal{X}}$ is singular. We claim that none of the points in its fiber under $\widetilde{\Pi}$ is defined over $\mathbb{F}_5$.

Suppose that this is not the case. Let P be an $\mathbb{F}_5$-rational point on $\widetilde{X}$ such that $\widetilde{\Pi}(P) = (4, 0)$. Let R be a point on $\widetilde{H}_5$ such that $\widetilde{\Phi}(R) = P$. Note that R has coordinates (c, d) such that

$$d^3 + 4d - 1 = 0, \qquad cd^2 + d + c^2 = 0, \qquad c^3 - 4c^2 - 1 = 0.$$

Now, over $\mathbb{F}_5$, we have the factorizations $d^3 + 4d - 1 = (d - 2)(d^2 + 2d + 3)$ and $c^3 - 4c^2 - 1 = (c-3)(c^2 - c + 2)$. Note that we cannot have $(c, d) = (3, 2)$, because then $cd^2 + d + c^2 \neq 0$. So we are left with three cases to consider:

Case 1: $d = 2$ and $c \neq 3$. Since P is $\mathbb{F}_5$-rational, the Galois conjugate $R^\sigma = (2/c, 2)$ of R satisfies $\widetilde{\Phi}(R^\sigma) = P$. In other words, R^σ is a $\langle \varrho \rangle$-conjugate of R, so it equals either $(1/2, c/2)$ or $(2/c, 1/c)$. Since $c \notin \mathbb{F}_5$, we get a contradiction.

Case 2: $d \neq 2$ and $c = 3$. As in the previous case, the Galois conjugate $R^\sigma = (3, 3/d)$ equals either $(1/d, 3/d)$ or $(d/3, 1/3)$. Since $d \notin \mathbb{F}_5$, we get a contradiction.

Case 3: $d \neq 2$ and $c \neq 3$. Note that $3d + 1$ is a root of the polynomial $T^2 - T + 2$, therefore, $c = 3d + 1$ or $c = -3d$. In the former case, we have $R^\sigma = (1 - 1/d, 3/d)$ and, as before, R^σ must equal either $(1/d, 3 + 1/d)$ or $(d/(3d + 1), 1/(3d + 1))$, a contradiction, since $d \notin \mathbb{F}_5$. In the latter case, $R^\sigma = (1/d, 3/d)$ and, as before, it must equal either $(1/d, -3)$ or $(-1/3, -1/3d)$, a contradiction, since $d \notin \mathbb{F}_5$. This proves the claim.

Therefore, there are exactly 6 $\mathbb{F}_5$-rational points on $\widetilde{X}$, so there are at most $6 + 2 = 8$ $\mathbb{Q}$-rational points on X. One of these points is the projection of a $\mathbb{Q}$-rational point on H_5, so it must be discarded. Therefore there are at most 7 $\mathbb{Q}$-rational points on X which lift to cubic points on H_5, so there are at most 21 cubic points on H_5, and this is our upper bound. As explained in [T3], the six known cubic points on H_5 (obtained by intersecting H_5 with the line $X + Y + Z = 0$ or the conic $XY + YZ + ZX = 0$) do not lift to cubic points on F_{13}. Hence, there are at most 15 cubic points on F_{13} and this completes the proof.

Acknowledgments. I thank Dino Lorenzini for encouraging me to use the effective Chabauty bounds given in [LT] in the context of [T2] and [T3] and for his comments on this work. I also thank the referee for his/her suggestions on a previous version of this manuscript.

References

[C] R. Coleman, *Effective Chabauty*, Duke Math. J. 52 (1985), 765–770.

[DK] O. Debarre and M. Klassen, *Points of low degree on smooth plane curves*, J. Reine Angew. Math. 446 (1994), 81–87.

[F] G. Faltings, *Diophantine approximation on abelian varieties*, Ann. of Math. 133 (1991), 549–576.

[GR] 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.

[KT] M. Klassen and P. Tzermias, *Algebraic points of low degree on the Fermat quintic*, Acta Arith. 82 (1997), 393–401.

[LT] D. Lorenzini and T. Tucker, *Thue equations and the method of Chabauty–Coleman*, Invent. Math. 148 (2002), 47–77.

[MT] W. McCallum and P. Tzermias, *On Shafarevich–Tate groups and the arithmetic of Fermat curves*, in: London Math. Soc. Lecture Note Ser. 303 (special volume in honor of P. Swinnerton-Dyer), Cambridge Univ. Press, 2003, 203–226.

[S] O. Sall, *Points algébriques de petit degré sur les courbes de Fermat*, C. R. Acad. Sci. Paris Sér. I. Math. 330 (2000), 67–70.

[T1] P. Tzermias, *Algebraic points of low degree on the Fermat curve of degree seven*, Manuscripta Math. 97 (1998), 483–488.

[T2] —, *Parametrization of low-degree points on a Fermat curve*, Acta Arith. 108 (2003), 25–35.

[T3] —, *Low degree points on Hurwitz–Klein curves*, Trans. Amer. Math. Soc. 356 (2004), 939–951.

Department of Mathematics
University of Tennessee
Knoxville, TN 37996-1300, U.S.A.
E-mail: tzermias@math.utk.edu

Received on 30.8.2004
and in revised form on 22.11.2004 (4840)