ACTA ARITHMETICA
108.1 (2003)

Parametrization of low-degree points on a Fermat curve

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 $\mathbb{Q}$. For a prime p such that $p \geq 5$, the *Fermat curve of degree* p is the smooth plane curve given by

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

Using results of Faltings ([Fl]), Debarre and Klassen ([DK]) showed that the set of algebraic points on F_p whose field of definition over $\mathbb{Q}$ has degree $d \leq p-2$ is finite. These points will be called *low-degree points* in the following. Debarre and Klassen asked whether all low-degree points on F_p lie on the line $X+Y+Z=0$. Thanks to Wiles and Taylor–Wiles, we can now exclude any discussion of the case $d=1$ in what follows. Thus, from now on, $d \geq 2$. The question of Debarre–Klassen was affirmatively resolved by Gross and Rohrlich ([GR]) for $p \leq 11$ and $d \leq (p-1)/2$, by Klassen and the author ([KT]) for $p=5$ and $d \leq 3$ and by the author ([T1]) for $p=7$ and $d \leq 5$. Note that the line $X+Y+Z=0$ is the unique line in the projective plane $\mathbb{P}^2$ which is invariant under the evident action of the symmetric group S_3 on $\mathbb{P}^2$. Note also that S_3 is a subgroup of the automorphism group of F_p for each p. The following weaker version of the question of Debarre–Klassen can be formulated:

QUESTION 1.1. If P is a low-degree point of degree $d \leq 6$ on F_p, is the Galois orbit of P contained in its S_3-orbit?

For $p \leq 7$, the answer is affirmative, as explained above. For $p \geq 13$, we refer the reader to [MT], where Question 1.1 is discussed and affirmatively established in special cases. In this paper, we discuss the case $p=11$. Our main result is the following theorem:

THEOREM 1.2. *There exist at most* 120 *points of degree* 6 *on* F_{11} *and the Galois orbit of each of these points equals its* S_3*-orbit.*

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

Combined with [GR], this shows that the answer to Question 1.1 is also affirmative for $p = 11$. The bound for points of degree 6 on F_{11} is obtained by means of Coleman's effective Chabauty method ([C]). It is not unlikely that such bounds can be obtained by the same method for any Fermat curve F_p for which Question 1.1 is affirmatively established. In Section 4, we produce an explicit curve C defined over $\mathbb{Q}$ whose $\mathbb{Q}$-rational points parametrize the Galois orbits of points of degree at most 6 on F_{11}.

2. Preliminary results. We follow Rohrlich's notation ([R]). Let ε be a primitive $2p$th root of unity in $\overline{\mathbb{Q}}$. The points at infinity on F_p are given by

$$a_j = (0, \varepsilon^{2j+1}, 1), \quad b_j = (\varepsilon^{2j+1}, 0, 1), \quad c_j = (\varepsilon^{2j+1}, 1, 0),$$

for $0 \le j \le p-1$. For convenience, let

$$\infty := c_{(p-1)/2} = (-1, 1, 0).$$

Let $K(F_p)$ be the field of rational functions on F_p. For an integer m let

$$\mathcal{L}(m\infty) = \{f \in K(F_p) : \operatorname{div}(f) \ge -m\infty\} \cup \{0\}.$$

Also consider the following elements of $K(F_p)$:

$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z}.$$

The following lemma is an easy consequence of the work of Rohrlich ([R]):

LEMMA 2.1. *If $k \in \{1, \ldots, p-2\}$, the rational functions $x^r/(x+y)^s$, where $0 \le r \le s \le k$, form a basis for the vector space $\mathcal{L}(pk\infty)$.*

Proof. If r and s are as in the lemma, then, by [R], we have

$$\operatorname{div}\left(\frac{x^r}{(x+y)^s}\right) = r\sum_{j=0}^{p-1} a_j - r\sum_{j=0}^{p-1} c_j - ps\infty + s\sum_{j=0}^{p-1} c_j \ge -ps\infty \ge -pk\infty.$$

It therefore suffices to show that

$$\dim(\mathcal{L}(pk\infty)) = \frac{(k+1)(k+2)}{2}.$$

It is well known (see for example [ACGH, p. 44]) that the Weierstrass gap sequence of ∞ is

$$1, 2, \ldots, p-2, p+1, p+2, \ldots, 2p-3, 2p+1, 2p+2, \ldots, 3p-4, \\ \ldots, (p-4)p+1, (p-4)p+2, (p-3)p+1.$$

This implies that

$$\dim(\mathcal{L}(p\infty)) = 3, \quad \dim(\mathcal{L}(p(k+1)\infty)) - \dim(\mathcal{L}(pk\infty)) = k+2$$

for $1 \le k \le p-3$, so the assertion follows by induction on k. ■

For the rest of the paper, let $p = 11$ and $k = 6$. Let J_{11} be the Jacobian variety of F_{11}. Fix a point P_1 of degree 6 on F_{11} and let P_i, where $1 \leq i \leq 6$, be the Galois conjugates of P_1. Then the divisor class

$$D = [P_1 + \ldots + P_6 - 6\infty]$$

is an element of $J_{11}(\mathbb{Q})$. Also consider the primitive pth root of unity $\zeta = \varepsilon^2$. Let us now recall some facts about the geometry of J_{11}. The reader should consult [Fd], [GR] and [KR] for a thorough account. The automorphisms A and B of F_{11} given by

$$A(X, Y, Z) = (\zeta X, Y, Z), \qquad B(X, Y, Z) = (X, \zeta Y, Z)$$

give rise to quotient curves of F_{11}. By a theorem of Faddeev ([Fd]), the Jacobians of three of these curves, namely

$$F_{11}/\langle AB^{-1}\rangle, \qquad F_{11}/\langle AB^{-5}\rangle, \qquad F_{11}/\langle AB^{-9}\rangle,$$

have finite Mordell–Weil group over $\mathbb{Q}$. By the work of Gross and Rohrlich ([GR]) it follows that

$$\sum_{j=0}^{10} (AB^{-t})^j D = 0$$

for $t \in \{1, 5, 9\}$. Therefore, for each t as above, there exists, by Lemma 2.1, a polynomial function $f_t(x, y)$ of degree 6 such that

$$\operatorname{div}\left(\frac{f_t(x, y)}{(x + y)^6}\right) = \sum_{j=0}^{10} (AB^{-t})^j (P_1 + \ldots + P_6) - 66\infty.$$

Thus, by [R],

$$\operatorname{div}(f_t(x, y)) = \sum_{j=0}^{10} (AB^{-t})^j (P_1 + \ldots + P_6) - 6\sum_{j=0}^{10} c_j.$$

Since F_{11} is a smooth plane curve, it follows that there exists a curve M_t of degree 6 in $\mathbb{P}^2$ which intersects F_{11} at the divisor

$$M_t.F_{11} = \sum_{j=0}^{10} (AB^{-t})^j (P_1 + \ldots + P_6).$$

Let $M_t : g_t(X, Y, Z) = 0$, where g_t is a homogeneous polynomial of degree 6.

LEMMA 2.2. *The polynomial g_t, where $t \in \{1, 5, 9\}$, can be written in the following form*:

(a) $g_1(X, Y, Z) = X^3Y^3 + \alpha X^2Y^2Z^2 + \beta XYZ^4 + \gamma Z^6$ *or* $Y^6 - \alpha X^5 Z$ *or* $X^6 - \alpha Y^5 Z$, *with* α, β, γ *in* $\mathbb{Q}$.

(b) $g_5(X, Y, Z) = X^3Z^3 + \alpha X^2Z^2Y^2 + \beta XZY^4 + \gamma Y^6$ *or* $Z^6 - \alpha X^5 Y$ *or* $X^6 - \alpha Z^5 Y$, *with* α, β, γ *in* $\mathbb{Q}$.

(c) $g_9(X,Y,Z) = Y^3Z^3 + \alpha Y^2Z^2X^2 + \beta YZX^4 + \gamma X^6$ *or* $Z^6 - \alpha Y^5 X$ *or* $Y^6 - \alpha Z^5 X$, *with* α, β, γ *in* $\mathbb{Q}$.

Proof. We will only prove part (a). The proof for the other two parts is similar (alternatively, parts (b) and (c) follow from part (a) if one uses the fact that the action of a 3-cycle of S_3 on J_{11} induces isomorphisms of the Jacobians of the three quotient curves of F_{11} defined above).

Let us first show that g_1 can be written as a polynomial with $\mathbb{Q}$-rational coefficients. Let σ be in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Note that $M_1.F_{11}$ is a $\mathbb{Q}$-rational divisor. Therefore, $M_1^\sigma.F_{11} = M_1.F_{11}$. We need to show that $M_1 = M_1^\sigma$. Suppose this is not the case. Since M_1 and M_1^σ have at least 66 points in common (their points of intersection with F_{11}), Bézout's theorem implies that they must have a common component C of maximum degree m with $1 \le m \le 5$. Write $M_1 = C + D$ and $M_1^\sigma = C + E$. Then $D.F_{11} = E.F_{11}$. Note that the degree of these intersection divisors equals $11(6-m)$. Therefore, the intersection of D and E contains at least $11(6-m) > (6-m)^2$ points, which contradicts Bézout's theorem and proves the rationality claim.

Also note that $M_1.F_{11}$ is a divisor invariant under AB^{-1}. By an argument similar to the rationality argument above, it follows that M_1 is invariant under AB^{-1}. As in the proof of Lemma 2.1 in [GR], write

$$g_1(X,Y,Z) = \sum_{0 \le i+j \le 6} a_{i,j} X^i Y^j Z^{6-i-j}.$$

Then M_1 is also described by the polynomial

$$AB^{-1}g_1(X,Y,Z) = g_1(\zeta X, \zeta^{-1}Y, Z) = \sum_{0 \le i+j \le 6} a_{i,j}\zeta^{i-j} X^i Y^j Z^{6-i-j}.$$

Hence, there exists $m \in \{0,1,\ldots,10\}$ such that $AB^{-1}g_1 = \zeta^m g_1$. Therefore, $a_{i,j} = 0$, unless $i - j \equiv m \pmod{11}$. Since $0 \le i, j, i+j \le 6$, we have the following cases to consider:

If $m = 0$ then $a_{i,j} = 0$, unless $i = j$. If we had $a_{3,3} = 0$ then g_1 would be divisible by Z, which contradicts the fact that no points at infinity can be in the support of $M_1.F_{11}$. Hence, $a_{3,3} \neq 0$ and g_1 can be written in the form $X^3Y^3 + \alpha X^2Y^2Z^2 + \beta XYZ^4 + \gamma Z^6$, with α, β, γ in $\mathbb{Q}$.

If $1 \le m \le 4$ then $a_{i,j} = 0$, unless $i = j + m$. Since $j + m \ge 1$, every nonzero monomial in g_1 is divisible by X, which, as before, is a contradiction.

If $m = 5$ then $a_{i,j} = 0$, unless $(i,j) \in \{(5,0),(0,6)\}$. If we had $a_{0,6} = 0$, then g_1 would be divisible by Y, which, as before, is a contradiction. Hence $a_{0,6} \neq 0$ and g_1 can be written in the form $Y^6 - \alpha X^5 Z$, with $\alpha \in \mathbb{Q}$.

If $m = 6$ then $a_{i,j} = 0$, unless $(i,j) \in \{(6,0),(0,5)\}$. As before, we see that g_1 can be written in the form $X^6 - \alpha Y^5 Z$, with $\alpha \in \mathbb{Q}$.

If $7 \leq m \leq 10$ then $a_{i,j} = 0$, unless $i - j = m - 11$. Since $11 + i - m \geq 1$, every non-zero monomial in g_1 is divisible by Y, which, as before, is a contradiction. ■

To facilitate our discussion, we make the following definition:

Definition 2.3. We say that M_1 (resp. M_5, M_9) is of *type I* if g_1 (resp. g_5, g_9) can be written in the first form stated in Lemma 2.2, part (a) (resp. (b), (c)). Otherwise, we say it is of *type II.*

We will now refine Lemma 2.2 (see Lemma 2.5 below). We will depend on the following well known fact (see for example [W], page 171):

Fact 2.4. If K is a number field, $a \in K$, q is a prime and $r \in \overline{\mathbb{Q}}$ is a root of the polynomial $T^q - a$ then either the field extension $K(r)/K$ has degree dividing q or $K(r) = K(\zeta_q)$, where ζ_q is a primitive qth root of unity in $\overline{\mathbb{Q}}$.

Lemma 2.5. *At most one of the curves M_1, M_5 and M_9 is of type II.*

Proof. Without loss of generality, assume that M_1 and M_5 are of type II. There are four cases to consider:

Case 1. Suppose that

$$g_1(X,Y,Z) = Y^6 - \alpha X^5 Z, \qquad g_5(X,Y,Z) = Z^6 - \beta X^5 Y,$$

with $\alpha, \beta \in \mathbb{Q}$. Write $P_1 = (1, c, d)$. Let L be the field of definition of P_1, i.e. $L = \mathbb{Q}(c,d)$. Since P_1 lies on both M_1 and M_5, we get

$$c^6 = \alpha d, \qquad d^6 = \beta c.$$

Therefore, $(cd)^5 \in \mathbb{Q}$. Since $[\mathbb{Q}(cd) : \mathbb{Q}]$ divides $[L : \mathbb{Q}] = 6$, Fact 2.4 implies that $cd \in \mathbb{Q}$, hence also $(cd)^{11} \in \mathbb{Q}$. But $c^{11} + d^{11} = -1 \in \mathbb{Q}$. Hence, there exists a quadratic extension K of $\mathbb{Q}$ such that $c^{11}, d^{11} \in K$. Since c and d are in L, degree considerations and Fact 2.4 imply that $c, d \in K$, which is impossible.

Case 2. Suppose that

$$g_1(X,Y,Z) = Y^6 - \alpha X^5 Z, \qquad g_5(X,Y,Z) = X^6 - \beta Z^5 Y,$$

with $\alpha, \beta \in \mathbb{Q}$. Write $P_1 = (c, d, 1)$ and let $L = \mathbb{Q}(c,d)$. Then

$$d^6 = \alpha c^5, \qquad c^6 = \beta d.$$

Therefore, $c^{31} \in \mathbb{Q}$. By Fact 2.4, we get $c \in \mathbb{Q}$, hence also $d \in \mathbb{Q}$, and this is impossible.

Case 3. Suppose that

$$g_1(X,Y,Z) = X^6 - \alpha Y^5 Z, \qquad g_5(X,Y,Z) = Z^6 - \beta X^5 Y,$$

with α, $\beta \in \mathbb{Q}$. Write $P_1 = (c, 1, d)$ and let $L = \mathbb{Q}(c,d)$. Then

$$c^6 = \alpha d, \qquad d^6 = \beta c^5.$$

Therefore, $c^{31} \in \mathbb{Q}$, so, as in the previous case, we reach a contradiction.

Case 4. Suppose that

$$g_1(X,Y,Z) = X^6 - \alpha Y^5 Z, \qquad g_5(X,Y,Z) = X^6 - \beta Z^5 Y,$$

with $\alpha, \beta \in \mathbb{Q}$. Write $P_1 = (c,d,1)$ and let $L = \mathbb{Q}(c,d)$. Then

$$c^6 = \alpha d^5, \qquad c^6 = \beta d.$$

Therefore, $d^4 \in \mathbb{Q}$. Let $K = \mathbb{Q}(d)$. Clearly, $[K : \mathbb{Q}] \le 4$. Note that since $c^6 = \beta d$, we get $c^6 \in K$. Since $c^{11} + d^{11} = -1$, we also have $c^{11} \in K$. Therefore, $c = (c^6)^2/c^{11}$ has to be in K, hence $L = K$, which is absurd, by degree. ∎

3. Galois action. In this section we prove the assertion about the Galois orbit of P_1 in Theorem 1.2. By Lemma 2.5, we may assume, without loss of generality, that both M_1 and M_5 are of type I. As before, write $P_1 = (c,d,1)$ and let $L = \mathbb{Q}(c,d)$.

Lemma 3.1. *The degree* $[\mathbb{Q}(cd) : \mathbb{Q}]$ *equals* 3.

Proof. Since $g_1(c,d,1) = 0$, the degree of cd over $\mathbb{Q}$ is at most 3. If it were at most 2, then both the sum and product of c^{11} and d^{11} are in a quadratic extension of $\mathbb{Q}$. So there exists a quartic extension K of $\mathbb{Q}$ containing both c^{11} and d^{11}. By Fact 2.4 and degree considerations we deduce that $c, d \in K$, which is impossible. ∎

Now note that g_1 is symmetric with respect to X and Y. Therefore, since $M_1.F_{11}$ contains the point $P_1 = (c,d,1)$, it must also contain the point $Q_1 = (d,c,1)$. Hence

$$(d,c,1) = Q_1 = (\zeta^m c^\sigma, \zeta^{-m} d^\sigma, 1),$$

for some integer m and some embedding $\sigma : L \hookrightarrow \overline{\mathbb{Q}}$. Therefore, $cd = (cd)^\sigma$, so σ fixes $\mathbb{Q}(cd)$. By Lemma 3.1, the extension $L/\mathbb{Q}(cd)$ has degree 2, so it is normal, which means that $L^\sigma = L$. But then $\zeta^m = d^\sigma/c$ is also in L. This can only happen if $\zeta^m = 1$. This shows that $Q_1 = P_1^\sigma$. Note also that if $Q_1 = P_1$ then c and d are 11th roots of $-1/2$, which is impossible since $[L : \mathbb{Q}] = 6$. Hence Q_1 equals P_i for some $i \in \{2, \ldots, 6\}$.

Similarly, note that g_5 is symmetric with respect to X and Z. By repeating the argument above, it follows that there exists an embedding $\tau : L \hookrightarrow \overline{\mathbb{Q}}$ such that $L^\tau = L$ and $R_1 := (1,d,c) = P_1^\tau$. Hence R_1 is also a Galois conjugate of P_1, different from P_1 and Q_1.

Note that the automorphisms σ and τ of L satisfy

$$c^\sigma = d, \qquad d^\sigma = c, \qquad c^\tau = 1/c, \qquad d^\tau = d/c.$$

Since $[L : \mathbb{Q}] = 6$, it easily follows that the orbit of P_1 under the group of automorphisms of L generated by σ and τ consists of the following six distinct elements:

$$P_1,\quad P_1^{\sigma},\quad P_1^{\tau},\quad P_1^{\sigma\tau}=(1,c,d),\quad P_1^{\tau\sigma}=(d,1,c),\quad P_1^{\sigma\tau\sigma}=(c,1,d).$$

These points are exactly the images of P_1 under the action of the subgroup S_3 of the automorphism group of F_{11} and our assertion is proved. Note that we have also shown that L is necessarily normal over $\mathbb{Q}$ with Galois group isomorphic to S_3 and generated by σ and τ. It is now easy to show that the curves M_1, M_5 and M_9 are all of type I, but we will not need this.

4. Explicit parametrization. Let C denote a smooth projective model of the curve obtained as the quotient of F_{11} by the action of S_3. Since the latter action is $\mathbb{Q}$-rational, it follows that C and the natural projection map $\phi : F_{11} \to C$ of degree 6 are also defined over $\mathbb{Q}$. Since we now know that the answer to Question 1.1 is affirmative for $p = 11$, it follows that the Galois orbits of points of degree at most 6 on F_{11} are in bijective correspondence with the $\mathbb{Q}$-rational points on C. Let J be the Jacobian of C.

Lemma 4.1. *The genus of C equals* 5 *and the Mordell–Weil rank of J over $\mathbb{Q}$ equals* 1.

Proof. Let g be the genus of C. Since the gonality of F_{11} (i.e. the minimum degree of a morphism $F_{11} \to \mathbb{P}^1$) equals 10, it follows that g cannot equal 0. Therefore, by Picard functoriality, ϕ induces an isogeny of J onto a non-trivial abelian subvariety of J_{11}. Since, by [KR], every absolutely simple isogeny factor of J_{11} has dimension 5, it follows that g is a positive multiple of 5. Now note that the genus of F_{11} equals 45. If R is the ramification divisor of ϕ the Riemann–Hurwitz formula gives $12g + \deg R = 100$, so $g \le 8$. Therefore, $g = 5$ and J is isogenous to one of the simple factors of J_{11}. By [GR], the Mordell–Weil rank of J over $\mathbb{Q}$ is at most 1. The fact that it equals 1 follows from the observation that the Gross–Rohrlich divisor class (see [GR]) is, up to torsion, invariant under the action of S_3, hence it induces a point of infinite order in $J(\mathbb{Q})$. ∎

Remark 4.2. The isogeny between J and a simple factor of J_{11} over $\mathbb{Q}$ is not an isomorphism. To see this, note that, by [GR], it suffices to show that $J(\mathbb{Q})$ has no element of exact order 11. Suppose D were such an element. The composite map

$$J \xrightarrow{\phi^*} J_{11} \xrightarrow{\phi_*} J$$

equals multiplication by 6 on J. Hence, $\phi_*(\phi^*(D)) \neq 0$, which is a contradiction, since, by [T2], $\phi^*(D)$ is supported on the three $\mathbb{Q}$-rational points on F_{11}. This implies that there is no non-constant morphism defined over $\mathbb{Q}$ from C to one of the Fermat quotient curves (since all these curves have genus 5, such a morphism would necessarily be an isomorphism). In particular, it does not seem likely that the $\mathbb{Q}$-rational points on the latter curves can be used to determine the $\mathbb{Q}$-rational points on C.

We will now produce an explicit model for C which will be used in the next section to give a bound for the number of points of degree 6 on F_{11}.

Proposition 4.3. *An affine model for C is given by*

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

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

$$\ominus : \mathbb{C}^2 \to \mathbb{C}^2 \quad \text{given by} \quad (x, y) \mapsto (r, s)$$

where

$$r = -x - y - \frac{1}{x} - \frac{1}{y} - \frac{x}{y} - \frac{y}{x} - 2,$$
$$s = xy + \frac{1}{xy} + \frac{x^2}{y} + \frac{y}{x^2} + \frac{y^2}{x} + \frac{x}{y^2} - 6.$$

Let $\mathcal{F}_{11}$ be the affine curve $x^{11} + y^{11} + 1 = 0$. It suffices to show that $\ominus$ induces, by restriction, a rational map $\psi : \mathcal{F}_{11} \to \mathcal{E}$ whose fiber above (r, s) equals

$$\{(x, y), (y, x), (1/x, y/x), (1/y, x/y), (y/x, 1/x), (x/y, 1/y)\}$$

for all but finitely many $(r, s) \in \mathcal{E}(\mathbb{C})$. 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

$$\begin{aligned}\ominus^{-1}(r, s) = \{&(x, y), (y, x), (1/x, y/x), (1/y, x/y), (y/x, 1/x), (x/y, 1/y), \\ &(1/x, 1/y), (1/y, 1/x), (x, x/y), (y, y/x), (x/y, x), (y/x, y)\}.\end{aligned}$$

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

$$cd = -\frac{(c + d) + (c + d)^2}{r + (c + d)}$$

and $c + d$ satisfies the following polynomial equation in T:

$$\begin{aligned}T^6 &+ (2r + 4)T^5 + (r^2 + 2r + 12 + s)T^4 + (16 + 6r + rs + 2s - 2r^2)T^3 \\ &+ (2rs + 8 + 11r + s - 3r^2 - r^3)T^2 + (rs + 8r - 2r^2)T + r^2 = 0.\end{aligned}$$

Thus there are at most six possible values for the pair $(c + d, cd)$, hence at most twelve possible values for the pair (c, d) and this proves the claim.

Now a straightforward but tedious calculation (which can be easily done using MAPLE) shows that

$$h(\ominus(x,y)) = -(x^{11}+y^{11}+1)(1/x^{11}+1/y^{11}+1).$$

In particular, ψ is a rational map from $\mathcal{F}_{11}$ to $\mathcal{E}$ and for $(r,s)\in\mathcal{E}(\mathbb{C})$ it follows that, for each $(x,y)\in\ominus^{-1}(r,s)$, either (x,y) or $(1/x,1/y)$ is on $\mathcal{F}_{11}$. Note that, with the exception of finitely many cases, only one of the latter two points can lie on $\mathcal{F}_{11}$. By the above calculation of the fibers of $\ominus$ and the evident symmetry of ψ, the assertion follows. ■

5. Consequences of the parametrization. Now we are ready to establish the bound stated in Theorem 1.2 on the number of points of degree 6 on F_{11}. Note that F_{11} has good reduction at 13, hence so does C. Let $\widetilde{C}$ denote a smooth projective model of the reduction of C at 13. By Lemma 4.1, Coleman's effective Chabauty method ([C]) applies and gives

$$\#C(\mathbb{Q}) \le \#\widetilde{C}(\mathbb{F}_{13}) + 8.$$

We first show that there are exactly 14 $\mathbb{F}_{13}$-rational points on $\widetilde{C}$. Let $\widetilde{F}_{11}$ be the reduction of F_{11} at 13. Also let $\widetilde{\mathcal{E}}$ denote the projectivization of the singular model of $\widetilde{C}$ obtained by reducing $\mathcal{E}$ at 13. 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 13. It is straightforward to check that $\widetilde{\mathcal{E}}$ has exactly 14 points defined over $\mathbb{F}_{13}$, namely the points (r,s) with coordinates $(1,0)$, $(1,1)$, $(1,3)$, $(1,6)$, $(2,11)$, $(3,8)$, $(4,5)$, $(4,12)$, $(5,11)$, $(8,10)$, $(10,2)$, $(10,9)$, $(12,8)$ and the unique point at infinity. Now each of the thirteen affine points listed above is a non-singular point of $\widetilde{\mathcal{E}}$, so its fiber under $\widetilde{\pi}$ consists of a unique $\mathbb{F}_{13}$-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 $\mathbb{F}_{13}$. To see this, note that any such point lifts under $\widetilde{\phi}$ to a point at infinity on $\widetilde{F}_{11}$ of degree at most 6 over $\mathbb{F}_{13}$. Since the cyclotomic polynomial of degree 10 remains irreducible over $\mathbb{F}_{13}$, it follows that the latter point has to equal $(0,-1,1)$, $(-1,0,1)$ or $(-1,1,0)$, which proves the claim.

Therefore, there are at most $14+8=22$ $\mathbb{Q}$-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 20 $\mathbb{Q}$-rational points on C which lift to points of degree 6 on F_{11}. Therefore, there are at most $20\cdot 6 = 120$ points of degree 6 on F_{11}. This completes the proof of Theorem 1.2.

We conclude the paper with the following proposition:

Proposition 5.1. *There are exactly six integral points of degree* 6 *on the affine subvariety* $x^{11}+y^{11}+1=0$ *of* F_{11}. *They all have the form* $(c,-1-c,1)$, *where* c *is a root of the irreducible polynomial*

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

Proof. Let $(c,d,1)$ be such a point and let $L=\mathbb{Q}(c,d)$. By Theorem 1.2, the norms of the algebraic integers c and d satisfy $N_{L/\mathbb{Q}}(c)=N_{L/\mathbb{Q}}(d)=1$, so c and d are units in L. Therefore, by the proof of Proposition 4.3, r and s are in $\mathbb{Z}$. Since r is an integer root of a monic polynomial with integer coefficients and constant term equal to -1, we get $r=-1$ or $r=1$. It is now straightforward to check that the only possibilities for (r,s) are $(1,0)$ and $(1,1)$. The former possibility gives $c^2+c+1=d^2+d+1=0$ (the Gross–Rohrlich points), which contradicts the assumption that L is of degree 6 over $\mathbb{Q}$. Hence $(r,s)=(1,1)$, which gives $c+d+1=0$. Thus $d=-c-1$, $L=\mathbb{Q}(c)$ and c is of degree 6 over $\mathbb{Q}$. The equation $c^{11}+d^{11}+1=0$ therefore implies that $c^6+3c^5+7c^4+9c^3+7c^2+3c+1=0$. ∎

Remark 5.2. Using valuation arguments, one can show that if (r,s) is a $\mathbb{Q}$-rational point on $\mathcal{E}$ then there exist pairwise coprime integers u, v and w such that either $r=\pm w^5v$, $s=u/(wv^2)$, with w not divisible by 11, or $r=\pm w^5/(11v)$, $s=u/(wv^2)$, with w divisible by 11. We have not been able to determine whether r and s are necessarily in $\mathbb{Z}$.

References

[ACGH] E. Arbarello, M. Cornalba, P. Griffiths and J. Harris, *Geometry of Algebraic Curves I*, Grundlehren Math. Wiss. 247, Springer, New York, 1985.

[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.

[Fd] D. Faddeev, *On the divisor class groups of some algebraic curves*, Soviet Math. Dokl. 2 (1961), 67–69.

[Fl] 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.

[KR] N. Koblitz and D. Rohrlich, *Simple factors in the Jacobian of a Fermat curve*, Canad. J. Math. 30 (1978), 1183–1205.

[MT] W. McCallum and P. Tzermias, *On Shafarevich–Tate groups of Fermat Jacobians*, preprint, 2002.

[R] D. Rohrlich, *Points at infinity on the Fermat curves*, Invent. Math. 39 (1977), 95–127.

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

[T2] P. Tzermias, *Torsion parts of Mordell–Weil groups of Fermat Jacobians*, Internat. Math. Res. Notices 1998, no. 7, 359–369.

[W] B. van der Waerden, *Modern Algebra*, Vol. I, revised edition, Frederick Ungar, New York, 1949.

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

Received on 6.5.2002
and in revised form on 8.7.2002 (4284)