Composito Mathematica **122:** 337–345, 2000.

Explicit Rational Functions on Fermat Curves and a Theorem of Greenberg

PAVLOS TZERMIAS
Department of Mathematics, P.O. Box 210089, 617 N. Santa Rita, The University of Arizona, Tucson, AZ 85721-0089, U.S.A. e-mail: tzermias@math.arizona.edu

(Received: 1 March 1999; accepted in final form: 25 August 1999)

Abstract. This paper is concerned with the arithmetic of curves of the form $v^p = u^s(1-u)$, where p is a prime with $p \geqslant 5$ and s is an integer such that $1 \leqslant s \leqslant p-2$. The Jacobians of these curves admit complex multiplication by a primitive p-th root of unity ζ. We find explicit rational functions on these curves whose divisors are p-multiples of divisors representing $(1-\zeta)^2$- and $(1-\zeta)^3$-division points on the corresponding Jacobians. This also gives an effective version of a theorem of Greenberg.

Mathematics Subject Classifications (2000): 11G30, 14G05.

Key words: Fermat curves, rational functions, Greenberg's theorem.

1 Introduction

Let $\mathbb{Q}$ be the field of rational numbers and let $\overline{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$. Let p be a fixed prime, such that $p \geqslant 5$, and let ϵ be a fixed primitive $2p$th root of unity in $\overline{\mathbb{Q}}$. Also define ζ by $\zeta = \epsilon^2$. Let K be the field $\mathbb{Q}(\zeta)$. For $s = 1, 2, \ldots, p-2$, let $F_{p,s}$ be a smooth projective model of the affine curve (defined over $\mathbb{Q}$)

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

Each $F_{p,s}$ is a curve of genus $(p-1)/2$ and its Jacobian $J_{p,s}$ admits complex multiplication induced by the automorphism ζ of $F_{p,s}$ defined by $(u, v) \mapsto (u, \zeta v)$. We define the endomorphism π of $J_{p,s}$ by $\pi = 1 - \zeta$. It is a well-known theorem of Greenberg [6] that the kernel of the endomorphism π^3 of $J_{p,s}$ is K-rational. In fact, combining Greenberg's result with the work of Coleman [1], Gross and Rohrlich [7] and Kurihara [8], one has the following theorem:

THEOREM 1. *Let p be a prime such that $p \geqslant 5$. For $s = 1, 2, \ldots, p-2$, we have $J_{p,s}[p^\infty](K) = J_{p,s}[\pi^3]$. Moreover, if l is a prime such that $l \neq p$, then $J_{p,s}[l^\infty](K) = \{0\}$, unless $l = 2$ and $(p, s) \in \{(7, 2), (7, 4)\}$.*

It should be noted that Theorem 1 is not effective, i.e. there is no systematic way known to produce explicit generators for the groups $J_{p,s}[\pi^2]$ or $J_{p,s}(K)_{\text{tors}}$ in general.

https://doi.org/10.1023/A:1002461930939 Published online by Cambridge University Press

Such generators are only known for the 'isomorphic' cases $(p, s) = (7, 2)$ and $(p, s) = (7, 4)$ (see [10]) and for the case $p = 5$ (see [2], [4] and [12]). Finding a non-trivial K-rational point on the curve which induces a torsion point on the Jacobian was crucial for settling the specific cases mentioned above. On the other hand, in view of the results of [3], such a point cannot exist for $p \geqslant 11$. It would be useful to have explicit information on the generators of $J_{p,s}[\pi^2]$ or $J_{p,s}(K)_{tors}$ in the general case. For example, in a recent paper [5], Grant used the 5-torsion on $J_{5,1}$ to construct a set of Abelian units which can be used to verify Rubin's conjecture in a case when the L-series has a second order zero at $s = 0$. Also, in [9], McCallum gave a general formula for the Cassels–Tate pairing on the π-torsion part of the Shafarevich–Tate group of $J_{p,s}$ over K. He noted that, for the formula to be applied directly, one needs to find an explicit rational function on $F_{p,s}$ whose divisor equals p times a divisor representing a π^2-torsion point on $J_{p,s}$. In the absence of such a function, McCallum used a p-adic approximation technique instead.

In this Letter, we construct such an explicit rational function on $F_{p,s}$. We also obtain a similar result for the case of π^3-torsion points on $J_{p,s}$. It should be noted that McCallum has a method (unpublished) that, given p and s, will construct such rational functions. Our approach is different and produces an explicit formula for all p and s. This also gives an effective version of Theorem 1, i.e. we get an algorithm that, given p and s, will, in principle, explicitly compute the associated divisors. We have used MAPLE to run this algorithm for the case of π^2-torsion points; this is discussed in more detail in the last section.

Our method is based on the fact that $F_{p,s}$ admits the Fermat curve F_p given by $X^p + Y^p + Z^p = 0$ as an unramified cover, whose Galois group is generated by the automorphism σ of F_p, where $\sigma(X, Y, Z) = (\zeta X, \zeta^{-s} Y, Z)$. We will use the Jacobian J_p of F_p to perform our calculations, by means of results of [11] and [13]. Denote by $f_{p,s} : F_p \to F_{p,s}$ the associated covering map. Depending on the context, we will use the same symbol $f_{p,s}$ to denote the induced maps $Div(F_p) \to Div(F_{p,s})$ and $J_p \to J_{p,s}$. Also, $f_{p,s}^*$ will be used to denote the dual maps $Div(F_{p,s}) \to Div(F_p)$ or $J_{p,s} \to J_p$ or the induced embedding of the function field of $F_{p,s}$ in the function field of F_p.

Consider the rational functions $x = X/Z$ and $y = Y/Z$ on F_p. Define

$$c = (-1)^{\frac{p-1}{2}} p^{-\frac{p+1}{2}} \prod_{j=1}^{p-1} (\zeta^j - 1)^j, \quad f(x, y) = c\left(x^{p-1} + \sum_{k=0}^{p-2}\left(x^{p-2-k} \prod_{l=1}^{k+1} (\epsilon - \zeta^l y)\right)\right).$$

Now consider the following functions on F_p:

$$h_1(x, y) = \frac{\epsilon - x}{y}, \qquad h_2(x, y) = (xy)^{\frac{s(1-p)}{2}} \prod_{j=0}^{s-1} f(x, \zeta^j y),$$

https://doi.org/10.1023/A:1002461930939 Published online by Cambridge University Press

$$g_m(x, y) = 1 + \sum_{k=0}^{p-2} \prod_{l=0}^{k} h_m(\zeta^{-l}x, \zeta^{ls}y),$$

for $m = 1, 2$. The rational functions $g_m(x, y)$ are not identically 0 on F_p (it can be shown that $g_2(-\zeta, 0) = g_1(\epsilon\zeta, 0) = 1$). Let *Norm* denote the norm map from the function field of F_p to that of $F_{p,s}$. Our main result is the following:

THEOREM 2. *Let p and s be as in Theorem 1. For $m = 1, 2$, there exists a divisor E_m on $F_{p,s}$ such that $pE_m = div(Norm(g_m(x, y)))$ and the divisor class of E_m generates the $\mathbb{Z}[\pi]$-module $J_{p,s}[\pi^{m+1}]$.*

Remark. Making use of the universal covering space of $\mathbb{C} - \{0, 1\}$, Rohrlich showed in [11] that the function $\prod_{j=1}^{p-1}((\epsilon\zeta^j - x)(\epsilon\zeta^j - y))^j$ has a pth root in the function field of F_p. The next proposition shows that $f(x, y)$ is such a pth root.

2. Auxiliary Results

PROPOSITION 1.

$$f(x, y)^p = \prod_{j=1}^{p-1}((\epsilon\zeta^j - x)(\epsilon\zeta^j - y))^j.$$

Proof. First we show that the polynomial $f(x, y)$ is symmetric in x, y. Since

$$f(0, y) = c\prod_{i=1}^{p-1}(\epsilon - \zeta^i y) = c\sum_{i=0}^{p-1}\epsilon^i\, y^{p-1-i} = f(y, 0),$$

the monomials y^r and x^r appear with the same coefficient in $f(x, y)$, for each $r \in \{1, \cdots, p-1\}$. Also, for $1 \leqslant s \leqslant r \leqslant p-2$, the coefficient of $x^{p-1-r}\, y^s$ in $f(x, y)$ equals

$$(-1)^s\, c\, \epsilon^{r-s} \sum_{1 \leqslant i_1 < \ldots < i_s \leqslant r} \zeta^{i_1} \ldots \zeta^{i_s}.$$

We claim that we have the following identities:

$$\sum_{1 \leqslant i_1 < \ldots < i_s \leqslant r} \zeta^{i_1} \ldots \zeta^{i_s} = \zeta^{\frac{s(s+1)}{2}} \prod_{j=r+1-s}^{r} (\zeta^j - 1) \prod_{j=1}^{s} (\zeta^j - 1)^{-1},$$

for $1 \leqslant s \leqslant r \leqslant p-2$. The claim is clearly true when $s = 1$ or $r = s$. Suppose it is true for $s \leqslant l$ or $s = l+1$ and $r = m$. Using the recursive formula

$$\sum_{1 \leqslant i_1 < \ldots < i_{l+1} \leqslant m+1} \zeta^{i_1} \ldots \zeta^{i_{l+1}} = \zeta^{m+1} \sum_{1 \leqslant i_1 < \ldots < i_l \leqslant m} \zeta^{i_1} \ldots \zeta^{i_l} + \sum_{1 \leqslant i_1 < \ldots < i_{l+1} \leqslant m} \zeta^{i_1} \ldots \zeta^{i_{l+1}}$$

and induction one sees that the claim is true for $s = l + 1$ and $r = m + 1$. The symmetry of $f(x, y)$ in x, y now follows from the equality

$$\zeta^{\frac{s(s+1)}{2}} \prod_{j=r+1-s}^{r} (\zeta^j - 1) = (-1)^s \, \zeta^{s(r+1)} \prod_{j=p-r}^{p-r+s-1} (\zeta^j - 1).$$

Now we can prove the equality in Proposition 1. First note that the two sides agree on $(0, \epsilon)$. This follows from the definition of the constant c and the relations

$$\overline{c} = (-1)^{\frac{p-1}{2}} \, c, \qquad c\overline{c} = p^{-1}, \qquad (D)$$

where $\overline{c}$ is the complex conjugate of c.

Now consider the points at infinity on F_p:

$$a_j = (0, \epsilon\zeta^j, 1), \qquad b_j = (\epsilon\zeta^j, 0, 1), \qquad c_j = (\epsilon\zeta^j, 1, 0),$$

for $0 \leqslant j \leqslant p - 1$. By Rohrlich's results in [11], it remains to show that

$$\mathrm{div}(f(x, y)) = \sum_{j=0}^{p-1} j \, (a_j + b_j) - (p-1) \sum_{j=0}^{p-1} c_j.$$

Looking at each summand in the definition of $f(x, y)$ and using [11], it follows that the order of $f(x, y)$ at a_j equals j, for all j. By the symmetry of $f(x, y)$ in x, y, we get that the order of $f(x, y)$ at b_j also equals j, for all j. Also by [11], the only possible poles of $f(x, y)$ are the points c_j, each of order at most $p - 1$. So the polar part of $\mathrm{div}(f(x, y))$ has degree at most $p(p - 1)$. On the other hand, by what has been said above, the degree of the zero part of $\mathrm{div}(f(x, y))$ is at least $p(p - 1)$. This completes the proof of Proposition 1.

LEMMA 1.

$$\prod_{l=0}^{p-1} h_1(\zeta^l x, \zeta^{-ls} y) = 1 = \prod_{l=0}^{p-1} h_2(\zeta^l x, \zeta^{-ls} y).$$

Proof. The first assertion is trivial. For the second assertion, note that, by Proposition 1,

$$\prod_{l=0}^{p-1} f(\zeta^l x, \zeta^{-ls} y)^p = \prod_{j=1}^{p-1} \prod_{l=0}^{p-1} ((\epsilon\zeta^j - \zeta^l x)(\epsilon\zeta^j - \zeta^{-ls} y))^j = \prod_{j=1}^{p-1} (xy)^{pj} = (xy)^{\frac{p^2(p-1)}{2}}.$$

Therefore, there exists an integer λ such that

$$\prod_{l=0}^{p-1} \frac{f(\zeta^l x, \zeta^{-ls} y)}{(xy)^{\frac{p-1}{2}}} = \zeta^{\lambda}.$$

https://doi.org/10.1023/A:1002461930939 Published online by Cambridge University Press

Now let $\phi(x, y) = (xy)^{(1-p)/2} f(x, y)$. Writing $\phi(x, y)$ in terms of the rational functions X/Y and Z/Y, it is easy to show that, for $0 \leqslant l \leqslant p-1$,

$$\phi(c_l)^2 = \zeta^{-l(l+1)}\ c^2 \left(\sum_{j=0}^{p-1} \zeta^{j^2}\right)^2 = \zeta^{-l(l+1)},$$

where the last equality follows from the classical theory of Gauss sums together with the relations (D) displayed in the proof of Proposition 1. Therefore,

$$\zeta^{2\lambda} = \prod_{l=0}^{p-1} \phi(c_l)^2 = 1,$$

so λ is divisible by p, and this implies the second assertion of Lemma 1.

3. Proof of Theorem 2

Consider the following divisors of degree 0 on F_p:

$$C_1 = \sum_{j=0}^{p-1} jb_j \ - \ \frac{p-1}{2} \sum_{j=0}^{p-1} b_j,$$

$$C_2 = \sum_{j=0}^{p-1} \frac{j(j+1)}{2} a_j \ - \ s \ \sum_{j=0}^{p-1} \frac{j(j+1)}{2} b_j \ + \frac{s(p-1)}{2} \sum_{j=0}^{p-1} jb_j - \frac{p+1}{2} \sum_{j=0}^{p-1} ja_j \ +$$

$$+ \frac{p^2-1}{12} \sum_{j=0}^{p-1} a_j \ - \frac{s(p-1)(p-5)}{12} \sum_{j=0}^{p-1} b_j.$$

Observe that $f_{p,s}(C_i) = 0$, for $i = 1, 2$. By parts (ii) and (iv) of Theorem 2 in [13], we get that

$$f_{p,s}^*(J_{p,s}[\pi^3]) = \langle C_1, C_2 \rangle, \qquad f_{p,s}^*(J_{p,s}[\pi^2]) = \langle C_1 \rangle. \qquad (E)$$

Note that, although the latter theorem was stated only for $p \geqslant 11$ in [13], its proof shows that it is still valid for $p = 5$; moreover, by substituting $J_{p,s}(K)_{tors}$ by $J_{p,s}[\pi^3]$ in the same proof, one sees that the equalities (E) also hold for $p = 7$.

LEMMA 2. *For $m = 1, 2$, the divisors $D_m = C_m + \mathrm{div}(g_m(x, y))$ satisfy the relation $\sigma(D_m) = D_m$.*

https://doi.org/10.1023/A:1002461930939 Published online by Cambridge University Press

Proof. Note that $\sigma(a_j) = a_{j-s}$ and $\sigma(b_j) = b_{j+1}$. A tedious calculation (using results of [11]) shows that

$$\sigma(C_1) - C_1 = \operatorname{div}(h_1(x, y)), \qquad \sigma(C_2) - C_2 = \operatorname{div}(h_2(x, y)).$$

Now, as in the proof of Hilbert's Theorem 90, Lemma 1 gives

$$h_m(x, y) = \frac{g_m(x, y)}{g_m(\zeta^{-1}x, \zeta^s y)},$$

for $m = 1, 2$. Since $\operatorname{div}(g_m(\zeta^{-1}x, \zeta^s y)) = \sigma(\operatorname{div}(g_m(x, y)))$, Lemma 2 follows.

Therefore, D_1 and D_2 are invariant under the group of automorphisms of F_p generated by σ. Since $F_{p,s}$ is the quotient of F_p by the latter group, there exist divisors E_m of degree 0 on $F_{p,s}$ such that $D_m = f^*_{p,s}(E_m)$, for $m = 1, 2$. Therefore, $f^*_{p,s}([E_m]) = [D_m] = [C_m]$. By the proof of Theorem 2 in [13], we have that $\operatorname{Ker}(f^*_{p,s}) = J_{p,s}[\pi]$. Therefore, by the displayed equalities (E), we see that $[E_m]$ generates the $\mathbb{Z}[\pi]$-module $J_{p,s}[\pi^{m+1}]$, for $m = 1, 2$. Moreover, by standard properties of coverings,

$$pE_m = f_{p,s}(f^*_{p,s}(E_m)) = f_{p,s}(D_m) = f_{p,s}(C_m) + f_{p,s}(\operatorname{div}(g_m(x, y)))$$

$$= f_{p,s}(\operatorname{div}(g_m(x, y))) = \operatorname{div}(\operatorname{Norm}(g_m(x, y))),$$

where the last equality follows from the fact that for a rational function g on F_p, the relation $f_{p,s}(\operatorname{div}(\sigma(g))) = f_{p,s}(\operatorname{div}(g))$ implies that $f_{p,s}(\operatorname{div}(g)) = \operatorname{div}(\operatorname{Norm}(g))$. This completes the proof of Theorem 2.

4. The Divisor E_1

In this Section, we discuss the problem of explicitly writing down the divisor E_1 of Theorem 2. By the previous Section, we only need to compute $\operatorname{div}(g_1(x, y))$. This will explicitly determine D_1 and hence also E_1 by the formula $D_1 = f^*_{p,s}(E_1)$, where $f_{p,s}((x, y)) = (u, v) = (-x^p, (-1)^{s-1}x^s y)$.

Clearly, any pole of $g_1(x, y)$ has to be a pole of $h_1(\zeta^{-l}x, \zeta^{ls}y)$, for some l such that $0 \leqslant l \leqslant p-2$. Therefore, by [11], the only possible poles of $g_1(x, y)$ are the points b_j, for $0 \leqslant j \leqslant p-1$ and

$$div\left(\prod_{l=0}^{k} h_1(\zeta^{-l}x, \zeta^{ls}y)\right) = (p-k-1)\sum_{j=0}^{k} b_j - (k+1)\sum_{j=k+1}^{p-1} b_j,$$

for $0 \leqslant k \leqslant p-2$. Hence, the polar part of $\operatorname{div}(g_1(x, y))$ equals $\sum_{j=1}^{p-1} j\, b_j$. Therefore, we only need to compute the zeros of $g_1(x, y)$. Using the change of variables $a = \epsilon/y$ and $b = -x/y$, we need to solve the following system of two polynomial equations in two unknowns a and b:

$$a^p + b^p = 1, \qquad 1 + \sum_{k=0}^{p-2} \prod_{l=0}^{k} (\zeta^{-ls}\, a + \zeta^{-l(s+1)}\, b) = 0.$$

We have used the Gröbner basis package in MAPLE to solve the above system for specific values of p and s. We list the output of the calculations in terms of the coordinates (u, v) of points in the support of E_1. The formulas $u = -b^p/a^p$, $v = -\epsilon^{s+1} b^s/a^{s+1}$ send (a, b) to (u, v).

$p = 5,\ s = 1$

$$(v + \zeta)(v + \zeta^2) = 0, \qquad u = (\zeta^2 - 1)\, v - (\zeta^2 + \zeta),$$

$$E_1 = \sum (u, v)\ - 2\ (1, 0).$$

Since the hyperelliptic involution $(u, v) \longmapsto (1 - u, v)$ of $F_{5,1}$ acts as multiplication by -1 on $J_{5,1}$, we get that the divisor class $[(-\zeta^2 - \zeta^3, -\zeta) - (1, 0)]$ generates $J_{5,1}[\pi^3]$ as a $\mathbb{Z}[\pi]$-module. This is the same divisor as in [2], [4] and [12].

$p = 7,\ s = 1$

$$v^3 + (-\zeta^5 + \zeta^2 + \zeta)\, v^2 + (\zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta)\, v - \zeta = 0,$$

$$u = (\zeta^4 + 2\zeta^3 + 2\zeta^2 + 2\zeta)\, v^2 + (\zeta^4 + \zeta^3 - \zeta - 1)\, v - (\zeta^3 + \zeta^2 + \zeta),$$

$$E_1 = \sum (u, v)\ - 3\ (1, 0).$$

$p = 7,\ s = 2$

$$v^3 + (1 - \zeta^5 - 2\zeta^4 - \zeta^3 + \zeta^2)\, v^2 + (1 - \zeta^4 - \zeta^3)\, v + 1 = 0,$$

$$u = (\zeta^5 - \zeta)\, v^2 + (\zeta^5 - \zeta)\, v + (\zeta^5 + \zeta^3 + 1),$$

$$E_1 = \sum (u, v)\ - 3\ (1, 0).$$

Prapavessi [10] showed that every point in $J_{7,2}(K)$ can be represented by a divisor of degree 0 supported on the Weierstrass points on $F_{7,2}$ (see also [1] where the Weierstrass points on $F_{7,2}$ are computed). The points (u, v) that we found above are not Weierstrass points.

$\underline{p = 11,\ s = 1}$

$$v^5 - (\zeta^9 + \zeta^8 + 2\zeta^7 + \zeta^6 + \zeta^5 - \zeta^2 - \zeta)\ v^4 + (\zeta^6 + 2\zeta^5 + 2\zeta^4 + 3\zeta^3 + 2\zeta^2 + 2\zeta + 1)\ v^3$$

$$+(\zeta^9 + \zeta^8 + 2\zeta^7 + 2\zeta^6 + 2\zeta^5 + 2\zeta^4 + 2\zeta^3 + 2\zeta^2 + \zeta + 1)\ v^2 - (\zeta + 1)\ v - \zeta^2 = 0,$$

$$u = -(\zeta^9 + 2\zeta^8 + \zeta^7 + \zeta^6 - \zeta^5 - 3\zeta^4 - 3\zeta^3 - 4\zeta^2 - 3\zeta - 2)\ v^4 +$$

$$+(\zeta^8 + 3\zeta^7 + 5\zeta^6 + 7\zeta^5 + 8\zeta^4 + 8\zeta^3 + 6\zeta^2 + 4\zeta + 2)\ v^3 +$$

$$+(\zeta^9 + 2\zeta^8 + 3\zeta^7 + 4\zeta^6 + 5\zeta^5 + 4\zeta^4 + 3\zeta^3 + \zeta^2 - 1)\ v^2 +$$

$$+(\zeta^8 + \zeta^7 + \zeta^6 + \zeta^5 - \zeta^3 - \zeta^2 - \zeta - 1)\ v - (\zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta),$$

$$E_1 = \sum (u, v) - 5\ (1, 0).$$

It would be interesting to recognize a precise pattern in the output of our calculations for the above cases; we have not been able to do so.

Acknowledgements

I thank Bill McCallum for his encouragement, Robert Coleman and David Grant for their interest in the problem and an anonymous referee for suggesting a number of improvements on the exposition. Part of this work was done during my stay at the Max Planck Institute in Bonn. I am indebted to Herbert Gangl and Ulf Kühn for introducing me to MAPLE.

References

1. Coleman, R.: Torsion points on abelian étale coverings of $\mathbb{P}^1 - \{0, 1, \infty\}$, *Trans. Amer. Math. Soc.* **311**(1) (1989), 185–208.
2. Coleman, R.: Torsion points on Fermat curves, *Compositio Math.* **58** (1986), 191–208.
3. Coleman, R., Tamagawa, A. and Tzermias, P.: The cuspidal torsion packet on the Fermat curve, *J. Reine Angew. Math.* **496** (1998), 73–81 .
4. Grant, D.: A proof of quintic reciprocity using the arithmetic of $y^2 = x^5 + 1/4$, *Acta Arith.* **75** (1996), 321–337.
5. Grant, D.: Units from 5-torsion on the Jacobian of $y^2 = x^5 + 1/4$ and the conjectures of Stark and Rubin, *J. Number Theory* (to appear).
6. Greenberg, R.: On the Jacobian variety of some algebraic curves, *Compositio Math.* **42** (1981), 345–359.
7. Gross, B. and Rohrlich, D.: Some results on the Mordell–Weil group of the Jacobian of the Fermat curve, *Invent. Math.* **44** (1978), 201–224.
8. Kurihara, M.: Some remarks on conjectures about cyclotomic fields and K-groups of $\mathbb{Z}$, *Compositio Math.* **81** (1992), 223–236.

9. McCallum, W.: On the Shafarevich-Tate group of the jacobian of a quotient of the Fermat curve, *Invent. Math.* **93** (1988), 637–666.
10. Prapavessi, D.: On the Jacobian of the Klein curve, *Proc. Amer. Math. Soc.* **122**(4) (1994), 971–978.
11. Rohrlich, D.: Points at infinity on the Fermat curves, *Invent. Math.* **39** (1977), 95–207.
12. Tzermias, P.: Arithmetic of cyclic quotients of the Fermat quintic, *Acta Arith.* **84**(4) (1998), 375–384.
13. Tzermias, P.: Torsion parts of Mordell–Weil groups of Fermat Jacobians, *Internat. Math. Res. Notices* (1998), No. 7, 359-369.