Functiones et Approximatio
46.1 (2012), 15–27
doi: 10.7169/facm/2012.46.1.2

ON CAUCHY-LIOUVILLE-MIRIMANOFF POLYNOMIALS II

Pavlos Tzermias

Abstract: The main result of [23] on the non-existence of low-degree irreducible factors of the Cauchy-Liouville-Mirimanoff polynomials $E_p(x)$ for primes $p \equiv 2 \pmod 3$ is extended to a similar result for $p \equiv 1 \pmod 3$. We also give a partial result on the existence of higher-degree irreducible factors.

Keywords: Cauchy-Liouville-Mirimanoff polynomials, factorization, Fermat curves, hypergeometric polynomials, ternary recurrences, powerful numbers.

1. Introduction

This paper is a continuation of [23]. For an integer $n \geqslant 2$, the following polynomial identity was known to Cauchy and Liouville ([4]):

$$(X+1)^n - X^n - 1 = X(X+1)^a(X^2+X+1)^b E_n(X), \tag{1.1}$$

where the so-called Cauchy-Liouville-Mirimanoff polynomial $E_n(X)$ has integer coefficients and a, b are defined as follows: if n even then $a = b = 0$, while if n is odd then $a = 1$ and $b = 0$, 1 or 2 according to whether $n \equiv 0$, 2 or 1 $\pmod 3$, respectively. For n prime, Mirimanoff ([12]) conjectured the irreducibility of $E_n(X)$ over $\mathbb{Q}$. It seems that $E_n(X)$ may in fact be irreducible for all n. This has already been established for several cases of composite n, namely when n is two times a prime by Filaseta (see Helou's paper [7]) and when n is three times a prime by Irick ([8]). Recently, Nanninga ([16]) has announced a proof for $n = 2^k m$ where m is an odd integer and $k \in \{1, 2, 3, 4, 5\}$. For an interesting variant of Mirimanoff's conjecture, we refer the reader to the work of Nicolas and Terjanian ([17], [21]).

Much less is known about Mirimanoff's conjecture for prime n. In this paper, we extend the main result of [23] on the non-existence of low-degree factors of $E_n(x)$ for prime $n \equiv 2 \pmod 3$ to a similar result for the case of prime $n \equiv 1 \pmod 3$. We also give a partial result on the existence of higher-degree factors of

2010 Mathematics Subject Classification: primary: 11R09, 12E30; secondary: 11G30, 11B37, 33A3

$E_n(X)$. In the process, the proofs of some of the results in [23] will be simplified, a new proof of a related classical polynomial identity will be given and some (not unexpected) connections to hypergeometric polynomials will be discussed. Our main results are the following theorems:

Theorem 1.1. *Let S be the set of primes greater than or equal to* 19 *and conguent to* 1 (mod 3). *There exists an effectively computable subset S_0 of S with S_0 having at most* 6 *elements and such that, for any p in $S \setminus S_0$, the polynomial $E_p(X)$ has no irreducible factor of degree $d \leqslant 11$ over $\mathbb{Q}$.*

For a real number x, let $\lfloor x \rfloor$ denote the integral part of x. Then:

Theorem 1.2. *Let p be a prime congruent to* 1 (mod 3). *Suppose that there exists a prime $q \geqslant 11$ such that $p \equiv 1 \pmod{q}$ and $p \not\equiv 1 \pmod{q^2}$. Then $E_p(X)$ has an irreducible factor of degree $d \geqslant 6\lfloor \frac{q}{3} \rfloor$ over $\mathbb{Q}$.*

Remark 1.3. The effectively computable set S_0 of possible exceptions in Theorem 1.1 arises from the general study of zeros of certain ternary recurrence sequences as carried out in the paper [11] by Mignotte, Shorey and Tijdeman. The effectively computable constants obtained in [11] are computed explicitly by Samaké in [20]. We have not been successful in using these bounds to perform an exhaustive calculation that could eliminate some or all of the possible exceptions. Our proof uses a crucial result of Beukers ([2]) obtained by methods of diophantine approximation. A list of all possible factors of $E_p(X)$ of degree at most 11 for $p \in S_0$ is also given.

Remark 1.4. As we show in the next section, thanks to the work of Helou ([7]), the problem of the non-existence of low-degree factors of $E_p(X)$ reduces to the problem of showing that certain polynomials have no integer roots. We show that these polynomials are in fact generalized hypergeometric polynomials of type ${}_3F_2$. This is neither unexpected nor difficult to prove. However, by a striking result of Wimp ([27]), no closed general formula exists for evaluating polynomials of type ${}_3F_2$ even at $x = 1$; a simpler proof of this fact has been given by Zeilberger in [29]. Therefore, it may not be too surprising that significant effort is needed to prove that the polynomials in question have no linear factors over $\mathbb{Q}$.

Remark 1.5. Theorem 1.2 would also be valid if we allowed q to equal 5 or 7, in which case its conclusion would be a triviality, in light of Helou's results ([7]) and Theorem 1.1. The reader may have recognized that the assumption involving q in Theorem 1.2 is a modified version of what it means for $p - 1$ to not be powerful in the sense of Golomb ([5]). In Section 4, we show that there are infinitely many p satisfying this assumption.

We also point out that our results can be restated in terms of low-degree points on Fermat curves (see also [6], [9], [10], [23], [24], [25], [26]):

Corollary 1.6. *Suppose that a point on the Fermat curve $X^p + Y^p = Z^p$ has degree $d \geqslant 2$ over $\mathbb{Q}$, lies on the line $X + Y = Z$ in $\mathbb{P}^2$ and is not of the form $(\eta, \frac{1}{\eta}, 1)$, where η is a primitive 6-th root of unity.*

(1) *If p is as in Theorem 1.1, then $d \geqslant 12$.*
(2) *If p and q are as in Theorem 1.2, then $d \geqslant 6\lfloor \frac{q}{3} \rfloor$.*

2. Some polynomial identities

Let n be an odd integer with $n \geqslant 9$. Let us briefly recall some known facts used in [23]. Helou ([7]) has shown that the set of roots of $E_n(X)$ is partitioned into orbits of cardinality 6 under a natural action of S_3 leaving the rational function

$$J = \frac{(X^2 + X + 1)^3}{(X^2 + X)^2} \tag{2.1}$$

invariant. It follows that there exists a polynomial $T_n(J) \in \mathbb{Q}[J]$ of degree r defined by $r = (n - 3 - 2b)/6$ such that

$$E_n(X) = n(X^2 + X)^{2r} T_n(J). \tag{2.2}$$

The factorization of $T_n(J)$ is closely related to that of $E_n(X)$. For instance, as Helou shows in [7], if n is prime, then $T_n(J)$ is a monic polynomial having integer coefficients, real and simple roots and the same number of irreducible factors as $E_n(X)$ over $\mathbb{Q}$. We give an explicit formula for $T_n(J)$:

Theorem 2.1. *For odd $n \geqslant 9$, we have*

$$T_n(J) = \sum_{m=0}^{r} \frac{1}{1 + 2r - 2m} \binom{m + b + 2r}{3m + b} J^m. \tag{2.3}$$

Proof. By Lemma 2.1 in [23], the polynomials $T_n(J)$ satisfy the recursion

$$\begin{aligned}(n + 18)&T_{n+18}(J) \\ &= (n + 12)(2J + 3)T_{n+12}(J) + (n + 6)(6J - J^2 - 3)T_{n+6}(J) + nT_n(J).\end{aligned}$$

It is a straightforward but tedious calculation to show that the sums on the right-hand side of (2.3) satisfy the same recursion. Alternatively, one can use the Maple package EKHAD implementing the powerful method of creative telescoping presented in the book by Petkŏvsek, Wilf and Zeilberger ([18]) to verify this. Also, the first few polynomials $T_n(J)$ are as follows (see [23]):

$$\begin{aligned}
T_9(J) &= J + \frac{1}{3} & T_{15}(J) &= J^2 + \frac{10}{3}J + \frac{1}{5} & T_{21}(J) &= J^3 + \frac{28}{3}J^2 + 7J + \frac{1}{7} \\
T_{11}(J) &= J + 1 & T_{17}(J) &= J^2 + 5J + 1 & T_{23}(J) &= J^3 + 12J^2 + 14J + 1 \\
T_{13}(J) &= J + 2 & T_{19}(J) &= J^2 + 7J + 3 & T_{25}(J) &= J^3 + 15J^2 + \frac{126}{5}J + 4.
\end{aligned}$$

Clearly, these polynomial expansions agree with the ones claimed in Theorem 2.1 and the proof is complete. ∎

The following result of Helou (see Lemma 3 in [7]) can also be derived from Theorem 2.1:

Corollary 2.2. *For prime $n \geqslant 11$, we have $T_n(J) \in \mathbb{Z}[J]$.*

Proof. Let n be prime. Then $b \neq 0$. We need to show that every coefficient of $T_n(J)$ is q-integral for all primes q. Fix a prime q. For $m \in \{0, \cdots, r\}$, the coefficient c_m of T^m in $J_n(J)$ satisfies

$$c_m = \frac{1}{1+2r-2m}\binom{m+b+2r}{2r-2m} = \frac{1}{m+b+2r+1}\binom{m+b+2r+1}{3m+b}. \quad (2.4)$$

If q does not divide $1+2r_n-2m$, then the q-adic valuation of c_m equals that of a binomial coefficent, hence it is non-negative. Suppose that q divides $1+2r-2m$. By (2.4), it suffices to show that q does not divide $m+b+2r+1$. If it did, then q would divide both $(m+b+2r+1)-(1+2r-2m) = 3m+b$ and $3(m+b+2r+1) = n+(3m+b)$, so q would divide n. Since n is prime, we get $q = n = 6r+3+2b$. Since q divides $3m+b$ and $3m+b \neq 0$ (because $b \neq 0$), it follows that $6r+3+2b \leqslant 3m+b$, which is impossible, because $m \leqslant r$. ∎

Remark 2.3. It is worth pointing out that Theorem 2.1 and Corollary 2.2 simplify the proofs of some results in [23], including the main result of [23], which follows by combining the result of Beukers ([2]) with the observation that for n prime with $n \equiv 2 \pmod 3$ the monic polynomial $T_n(J) \in \mathbb{Z}[J]$ is not reciprocal and has constant coefficient 1. Note also that in this case the Newton polygon of $T_n(J)$ with respect to any prime consists of a single horizontal edge, therefore no factorization information can obtained that way. Finally, Lemma 2.2 in [23] immediately follows from (2.3); combined with Lemma 3 in Helou's paper ([7]), this shows that $T_n(J)$ is a Hurwitz polynomial for all odd $n \geqslant 9$.

The following polynomial identity is classical. According to Ribenboim ([19]), it first appeared in Todhunter's book ([22]). Other proofs were given by Muir ([15]), Carlitz and Hunter ([3]) and Wituła and Słota ([28]). For an interesting generalization, the reader should also consult the paper by Mostafa ([13]). We use Theorem 2.1 to give yet another proof of this identity. We caution the reader that there is a misprint in the formula given in [19] (formula (2E), page 227) and in [13] (page 424), as the proofs in [19] (pages 227-229) clearly demonstrate.

Theorem 2.4. *Let $U = x^2+xy+y^2$ and $V = xy(x+y)$. For odd $n \geqslant 9$, we have*

$$(x+y)^n - x^n - y^n = \sum_{k=\frac{n+b-3}{3}}^{\frac{n-3}{2}} \frac{n}{n-2-2k}\binom{k}{n-3-2k} U^{3k-n+3} V^{n-2k-2}.$$

Proof. By (2.1) and Theorem 2.1, we have

$$T_n\left(\frac{(X^2+X+1)^3}{(X^2+X)^2}\right) = \sum_{m=0}^{r} \frac{1}{1+2r-2m}\binom{m+b+2r}{3m+b}\frac{(X^2+X+1)^{3m}}{(X^2+X)^{2m}},$$

so, by (1.1) and (2.2), we get

$$(X+1)^n - X^n - 1 = \sum_{m=0}^{r} \frac{n}{1+2r-2m} \binom{m+b+2r}{3m+b} \frac{(X^2+X+1)^{3m+b}}{(X^2+X)^{2m-1-2r}}.$$

Letting $k = m + \frac{n+b-3}{3}$, we get

$$(X+1)^n - X^n - 1 = \sum_{k=\frac{n+b-3}{3}}^{\frac{n-3}{2}} \frac{n}{n-2-2k} \binom{k}{n-3-2k} \frac{(X^2+X+1)^{3k-n+3}}{(X^2+X)^{2k+2-n}}.$$

Finally, replacing X by $\frac{x}{y}$ and multiplying through by y^n completes the proof. ■

As discussed in Remark 1.4, $T_n(J)$ can be expressed as a generalized hypergeometric polynomial of type ${}_3F_2$ (for a wealth of information on the properties of such functions we refer the reader to the book by Andrews, Askey and Roy [1]). Note that exactly two of the numbers $\frac{b+1}{3}$, $\frac{b+2}{3}$, $\frac{b+3}{3}$ are not integers. Let α, β denote these two numbers. Specifically, $\{\alpha, \beta\}$ equals $\{\frac{1}{3}, \frac{2}{3}\}$, $\{\frac{2}{3}, \frac{4}{3}\}$ or $\{\frac{4}{3}, \frac{5}{3}\}$ depending on whether b equals 0, 1 or 2, respectively. Then

Corollary 2.5. *Let notation be as above. For odd $n \geqslant 9$, we have*

$$T_n(J) = \frac{1}{1+2r} \binom{b+2r}{b} \, {}_3F_2\left(b+2r+1, -r, -\frac{1}{2}-r \; ; \; \alpha, \beta \; ; \; \frac{4}{27}J\right).$$

Proof. For a positive integer m and a real number x, let $(x)_m$ denote the Pochhammer symbol of x, i.e. $(x)_m = x(x+1)\cdots(x+m-1)$. Also let $(x)_0 = 1$. Let c_m be the coefficient of J^m in (2.3). For $m \in \{0, \cdots, r-1\}$, we have

$$\begin{aligned} \frac{c_{m+1}}{c_m} &= \frac{(m+1+b+2r)(2r-2m)(2r-2m+1)}{(3m+1+b)(3m+2+b)(3m+3+b)} \\ &= \frac{4}{27} \frac{(m+1+b+2r)(m-r)(m-\frac{1}{2}-r)}{(m+\frac{b+1}{3})(m+\frac{b+2}{3})(m+\frac{b+3}{3})}. \end{aligned}$$

Therefore, by definition of $\{\alpha, \beta\}$,

$$c_{m+1} = c_0 \prod_{i=0}^{m} \frac{c_{i+1}}{c_i} = c_0 \frac{(b+2r+1)_{m+1} \; (-r)_{m+1} \; (-\frac{1}{2}-r)_{m+1}}{(\alpha)_{m+1} \; (\beta)_{m+1} \; (m+1)!} \left(\frac{4}{27}\right)^{m+1},$$

and the result follows from Theorem 2.1. ■

3. Low-degree factors

For the rest of this paper, we will only be concerned with the case when n is prime with $n \equiv 1 \pmod 3$. For simplicity, we denote n by p. Write $p = 6t+1$, for some integer $t > 1$. Note that in this case we have $b = 2$ and $r = t-1$. Also note that

$$\frac{1}{2t-2m-1} \binom{2t+m}{3m+2} = \frac{(2t+m)!}{(3m+2)!(2t-2m-1)!} = \frac{1}{3m+2} \binom{2t+m}{3m+1}.$$

Therefore, (2.3) now reads as follows:

$$T_p(J) = \sum_{m=0}^{t-1} \frac{1}{3m+2}\binom{2t+m}{3m+1} J^m. \tag{3.1}$$

In particular, $T_p(J)$ is monic with constant coefficient t. For $0 \leqslant m \leqslant t-1$, let c_m be the coefficient of J^m in (3.1). For a prime q and a positive integer x, let $v_q(x)$ denote the q-adic valuation of x. Before we prove Theorem 1.1, we need to establish some auxiliary results:

Lemma 3.1. *If q is a prime and m is a positive integer, then*

$$v_q((3m+2)!) \leqslant \begin{cases} 3m+1 & \text{if } q=2 \\ \left\lfloor \frac{3m}{2} \right\rfloor & \text{if } q=3 \\ m & \text{if } q=5 \\ \left\lfloor \frac{2m}{3} \right\rfloor & \text{if } q \geqslant 7 \end{cases}.$$

Proof. For a positive integer x, let $\sigma_q(x)$ denote the sum of the digits in the expansion of x in base q. By a classical theorem of Legendre, we have

$$v_q(x!) = \frac{x - \sigma_q(x)}{q-1}.$$

Therefore, $v_2((3m+2)!) \leqslant 3m+1$ and $v_5((3m+2)!) \leqslant \frac{3m+1}{4} \leqslant m$. Also, for $q \geqslant 7$, we have $v_q((3m+2)!) \leqslant \frac{3m+1}{q-1} \leqslant \frac{3m+1}{6} \leqslant \frac{2m}{3}$, so $v_q((3m+2)!) \leqslant \lfloor \frac{2m}{3} \rfloor$. Finally, since $3m+2$ is not a power of 3, we get $\sigma_q(3m+2) \geqslant 2$, hence $v_3((3m+2)!) \leqslant \frac{3m}{2}$, so $v_3((3m+2)!) \leqslant \lfloor \frac{3m}{2} \rfloor$. ∎

For an integer $m \in \{1, \cdots, t-2\}$, define

$$b_m = 2(2t+m)\cdots(2t+1)(2t-1)\cdots(2t-2m). \tag{3.2}$$

By (3.1), we get

$$c_m = \frac{t\ b_m}{(3m+2)!}. \tag{3.3}$$

Lemma 3.2. *For $1 \leqslant m \leqslant t-2$, we have*

$$\left\lfloor \frac{5m}{3} \right\rfloor \ + \ v_2(b_m) \ \geqslant \ v_2((3m+2)!).$$

Proof. For $m=1$, we have $\lfloor \frac{5}{3} \rfloor = 1$, $b_1 = 4(2t+1)(2t-1)(t-1)$ and $v_2(120) = 3$, so the inequality holds. Suppose now that $m \geqslant 2$. Note that exactly $\lfloor \frac{m}{2} \rfloor$ of the integers $2t+1, \cdots, 2t+m$ and exactly m of the integers $2t-1, \cdots, 2t-2m$ are even. Hence, $v_2(b_m) \geqslant 1 + m + \lfloor \frac{m}{2} \rfloor$. By Lemma 3.1, it suffices to show that $1 + m + \lfloor \frac{m}{2} \rfloor + \lfloor \frac{5m}{3} \rfloor \geqslant 3m+1$, i.e. that

$$2m \leqslant \left\lfloor \frac{m}{2} \right\rfloor + \left\lfloor \frac{5m}{3} \right\rfloor. \tag{3.4}$$

We write $m = 6k + l$, with $k \in \mathbb{Z}$ and $0 \leqslant l \leqslant 5$, and check all cases:

If $l = 0$, then (3.4) reads $12k \leqslant 3k + 10k$, which is true.

If $l = 1$, then $k \geqslant 1$ (since $m \geqslant 2$) and (3.4) reads $12k + 2 \leqslant 3k + 10k + 1$, which is true.

If $l = 2$, then (3.4) reads $12k + 4 \leqslant 3k + 1 + 10k + 3$, which is true.

If $l = 3$, then (3.4) reads $12k + 6 \leqslant 3k + 1 + 10k + 5$, which is true.

If $l = 4$, then (3.4) reads $12k + 8 \leqslant 3k + 2 + 10k + 6$, which is true.

If $l = 5$, then (3.4) reads $12k + 10 \leqslant 3k + 2 + 10k + 8$, which is true. ■

For $1 \leqslant m \leqslant t - 2$ and a prime q, define

$$e_q(m) = \begin{cases} \lfloor \frac{5m}{3} \rfloor & \text{if } q = 2 \\ \lfloor \frac{3m}{2} \rfloor & \text{if } q = 3 \\ m & \text{if } q = 5 \\ \lfloor \frac{2m}{3} \rfloor & \text{if } q \geqslant 7 \end{cases}.$$

The following lemma is an immediate consequence of Lemmas 3.1 and 3.2:

Lemma 3.3. *For $1 \leqslant m \leqslant t - 2$, we have*

$$\frac{b_m}{(3m+2)!} \prod_{\substack{q \leqslant 3m+2 \\ q \text{ prime}}} q^{e_q(m)} \in \mathbb{Z}.$$

Now, by Helou's results ([7]), specifically the fact that every irreducible factor of $E_p(X)$ has degree a multiple of 6, it follows that the proof of Theorem 1.1 reduces to finding all rational roots of $T_p(J)$. Since the polynomial $T_p(J) \in \mathbb{Z}[J]$ is monic with positive coefficients and constant term t, every rational root of $T_p(J)$ must be of the form $-w$, for some positive integer w dividing t. Fix such a root.

Lemma 3.4. *For $m \in \{1, \cdots, t-2\}$, we have*

$$w^{m+1} \mid t \prod_{\substack{q \leqslant 3m+2 \\ q \text{ prime}}} q^{e_q(m)}.$$

Proof. We use induction on m. Let $m = 1$. Since $T_p(-w) = 0$, we get $w^2 \mid (-w)c_1 + c_0$, so $w^2 \mid 30(-w)c_1 + 30c_0$. By (3.1), we have

$$w^2 \mid (-w)(2t+1)(2t-1)(t-1)t + 30t.$$

Since $w \mid t$, it follows that $w^2 \mid 30t$, so the lemma is true for $m = 1$. Suppose that it is true for all m with $1 \leqslant m < M \leqslant t - 2$. We need to show that it is true for $m = M$. Since $T_p(-w) = 0$, we have

$$w^{M+1} \mid \sum_{m=0}^{M} c_m \, (-w)^m.$$

Therefore,

$$w^{M+1} \mid \sum_{m=0}^{M} \left(\prod_{\substack{q \leqslant 3M+2 \\ q \text{ prime}}} q^{e_q(M)} \right) c_m (-w)^m.$$

Since $c_0(-w)^0 = t$, we will be done if we can show that

$$w^{M+1} \mid \sum_{m=1}^{M} \left(\prod_{\substack{q \leqslant 3M+2 \\ q \text{ prime}}} q^{e_q(M)} \right) c_m (-w)^m,$$

which, by (3.3), can be written as

$$w^{M+1} \mid \sum_{m=1}^{M} \left(\prod_{\substack{q \leqslant 3M+2 \\ q \text{ prime}}} q^{e_q(M)} \right) \frac{b_m}{(3m+2)!} (-w)^m t.$$

Using Lemma 3.3 and the fact that $w \mid t$, it suffices to show that

$$w^{M+1} \mid \sum_{m=1}^{M-1} \left(\prod_{\substack{q \leqslant 3M+2 \\ q \text{ prime}}} q^{e_q(M)} \right) \frac{b_m}{(3m+2)!} (-w)^m t.$$

It would be enough to show that each of the summands above is divisible by w^{M+1}, i.e. that for $1 \leqslant m \leqslant M-1$, we have

$$w^{M-m+1} \mid \left(\prod_{\substack{q \leqslant 3M+2 \\ q \text{ prime}}} q^{e_q(M)} \right) \frac{b_m}{(3m+2)!} t.$$

By Lemma 3.3, it suffices to show that for $1 \leqslant m \leqslant M-1$, we have

$$w^{M-m+1} \mid t \prod_{\substack{q \leqslant 3M+2 \\ q \text{ prime}}} q^{e_q(M) - e_q(m)}.$$

Since $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x+y \rfloor$ for all real numbers x, y, we easily see that $e_q(M) - e_q(m) \geqslant e_q(M-m)$, for all primes q, so it suffices to show that

$$w^{M-m+1} \mid t \prod_{\substack{q \leqslant 3M+2 \\ q \text{ prime}}} q^{e_q(M-m)},$$

which follows from the induction hypothesis and completes the proof. ∎

We are now ready to prove Theorem 1.1:

Proof of Theorem 1.1. Since $E_{19}(X)$ is irreducible over $\mathbb{Q}$, we may assume $p \geqslant 31$, hence $t \geqslant 5$. Using $m = t-2$ in Lemma 3.4 gives

$$w^{t-1} \mid t \prod_{\substack{q \leqslant 3t-4 \\ q \text{ prime}}} q^{e_q(t-2)}. \tag{3.5}$$

Suppose that w is divisible by some prime $l > 3t-4$. Then $l \geqslant 11$ and l^{t-1} divides t, so $t \geqslant l^{t-1} \geqslant 11^{t-1}$, a contradiction. Therefore, w is only divisible by primes $q \leqslant 3t-4$. By (3.5), we get

$$(t-1)v_q(w) \leqslant v_q(t) + e_q(t-2), \tag{3.6}$$

for all primes $q \leqslant 3t-4$.

If $v_2(w) \geqslant 2$, then (3.6) gives

$$v_2(t) \geqslant 2(t-1) - \left\lfloor \frac{5t-10}{3} \right\rfloor \geqslant 2t - 2 - \frac{5t-10}{3} = \frac{t+4}{3},$$

so $2^{\frac{t+4}{3}} \leqslant t$, a contradiction. Therefore, $v_2(w) \leqslant 1$.

If $v_3(w) \geqslant 2$, then (3.6) gives

$$v_3(t) \geqslant 2t - 2 - \left\lfloor \frac{3t-6}{2} \right\rfloor \geqslant 2t - 2 - \frac{3t-6}{2} = \frac{t+2}{2},$$

so $3^{\frac{t+2}{2}} \leqslant t$, a contradiction. Therefore, $v_3(w) \leqslant 1$.

If $v_5(w) \geqslant 2$, then (3.6) gives $v_5(t) \geqslant 2t - 2 - (t-2) = t$, so $5^t \leqslant t$, a contradiction. Therefore, $v_5(w) \leqslant 1$.

Let q be a prime such that $7 \leqslant q \leqslant 3t-4$. If $v_q(w) \geqslant 1$, then (3.6) gives

$$v_q(t) \geqslant t - 1 - \left\lfloor \frac{2t-4}{3} \right\rfloor \geqslant t - 1 - \frac{2t-4}{3} = \frac{t+1}{3},$$

so $t \geqslant q^{\frac{t+1}{3}} \geqslant 7^{\frac{t+1}{3}}$, a contradiction. Therefore, $v_q(w) = 0$.

The conclusion from analyzing the above cases is that w necessarily divides $30 = 2 \cdot 3 \cdot 5$, so the only possible values of w are 1, 2, 3, 5, 6, 10, 15 and 30. By a crucial result of Beukers ([2]), the polynomials $E_n(X)$ are pairwise relatively prime for $n \geqslant 2$, hence the same is true for the polynomials $T_n(J)$, for odd $n \geqslant 9$. Since -1 is a root of $T_{11}(J)$ and -2 is a root of $T_{13}(J)$, it follows that w can only be in $\{3, 5, 6, 10, 15, 30\}$ and also that for each of these values of w, there is at most one prime $p \in S$ such that $-w$ is a root of $T_p(J)$. This forms the subset S_0 in the statement of Theorem 1.1. Moreover, S_0 is effectively computable: replacing J by the six possible values of $-w$ in the ternary recursion used in the proof of Theorem 2.1 produces six explicit ternary recurrence sequences of integers satisfying the assumptions of Theorem 1 in the paper of Mignotte,

Shorey and Tijdeman ([11]). Therefore, the zeros of these recurrence sequences are effectively computable and can be explicitly computed as in Samaké's thesis ([20]). As mentioned in Remark 1.3, we have not been able to perform the exhaustive calculation needed to decide if any (or all) of the at most six possible exceptions can be eliminated. For the sake of completeness, we also mention that, by formula (3) in Helou's paper ([7]), every possible factor of degree $\leqslant 11$ of $E_p(X)$ for $p \in S_0$ is of the form

$$X^6 + 3X^5 + (w+6)X^4 + (2w+7)X^3 + (w+6)X^2 + 3X + 1,$$

for $w \in \{3, 5, 6, 10, 15, 30\}$. ■

4. Higher-degree factors

In this section, we discuss higher-degree irreducible factors of $E_p(J)$ (equivalently, non-linear irreducible factors of $T_p(J)$). Newton polygons will be our main tool; we follow the terminology in the paper by Mott ([14]).

We first note that $T_p(J)$ never satisfies Eisenstein's irreducibility criterion:

Lemma 4.1. *The greatest common divisor of the coefficients c_0, c_1 and c_{t-2} equals 1. In particular, $T_p(J)$ is not q-Eisenstein for any prime q.*

Proof. From (3.1), we have

$$c_0 = t, \quad c_1 = \frac{(2t+1)(2t-1)(t-1)t}{30}, \qquad c_{t-2} = \frac{(t-1)(3t-2)}{2}.$$

Suppose that there exists a common prime divisor q of c_0, c_1 and c_{t-2}. Then q divides t and $(t-1)(3t-2)$. Since $(t, t-1) = 1$, it follows that q divides t and $3t-2$, hence $q = 2$. If $t \equiv 2 \pmod 4$, then c_1 is odd, a contradiction. If 4 divides t, then c_{t-2} is odd, a contradiction. ■

The following example illustrates that, for certain p, the existence of even a single non-linear irreducible factor of $T_p(J)$ cannot be derived from the shape of any Newton polygon of $T_p(J)$:

Example 4.2. Let $p = 61$. We have $t = 10$. The Newton polygon of $T_p(J)$ with respect to any prime $q \neq 2, 5$ consists of a single horizontal edge. The Newton polygon with respect to either $q = 2$ or $q = 5$ consists of a horizontal edge of width $t-2$ together with an edge of width 1 and slope 1. Therefore, higher-degree irreducible factors of $T_p(J)$ are not "visible" in any of its Newton polygons.

Hence, it seems unlikely that an unconditional version of Theorem 1.2 can be obtained on the basis of Newton polygons alone. We now proceed with the proof of Theorem 1.2:

Proof of Theorem 1.2. Since $t = \frac{p-1}{6}$ and $q \neq 2, 3$, we see that q divides t but q^2 does not divide t. Let $m = \lfloor \frac{q}{3} \rfloor$. Then $3m \leqslant q \leqslant 3m+2$. Therefore, $v_q((3m+2)!) = 1$ and q does not divide $(3k+2)!$ for any $k \leqslant m-1$. By (3.1),

$$c_k = \frac{(2t+k)\cdots(2t+1)2t(2t-1)\cdots(2t-2k)}{(3k+2)!}.$$

It follows that q divides $c_0, \cdots, c_{m-1}$ and $v_q(c_m) = 0$ (because q does not divide $2t-1, \cdots, 2t-2k, 2t+1, \cdots, 2t+k$). Therefore, the last edge of the Newton polygon of $T_p(J)$ with respect to q is in fact a segment of width m and height 1. By a standard argument (e.g. Corollary 2.5 in [14]), we get that some irreducible factor of $T_p(J)$ has degree $\geqslant m$ and, by [7], Theorem 1.2 follows. ■

We conclude this paper by showing that there are infinitely many primes p satisfying the conditions of Theorem 1.2. The proof is based on a variation of the argument used by Golomb ([5]) to compute the density of powerful numbers.

Lemma 4.3. *There are infinitely many primes p satisfying the hypotheses of Theorem* 1.2.

Proof. For a set T, let $\#T$ denote the number of elements in T. For an integer $x \geqslant 2$, consider the following sets:

$$\begin{aligned}
A(x) &= \{n \in \{1, \cdots, x\} : \forall \text{ primes } q \geqslant 11,\ q \mid n \Rightarrow q^2 \mid n\},\\
B(x) &= \{1, \cdots, x\} \setminus A(x),\\
C(x) &= \{n \in \{1, \cdots, x\} : n \text{ is prime }, \ n \equiv 1 \pmod 3\},\\
D(x) &= \{n \in \{1, \cdots, x\} : n - 1 \in B(x)\}.
\end{aligned}$$

Clearly, $\#D(x) = \#B(x-1)$. Also, by Dirichlet's theorem on primes in arithmetic progressions and the prime number theorem, there exists a positive constant C_1 such that $\#C(x) \geqslant C_1 \frac{x}{\ln(x)}$. Now, any number n in $A(x)$ can be uniquely written in the form $n = lk^2m^3$, where l can only be divisible by primes in $\{2, 3, 5, 7\}$, k and m are relatively prime to $210 = 2 \cdot 3 \cdot 5 \cdot 7$ and m is square-free (take m to be the product of all primes $\geqslant 11$ appearing with odd exponent in the prime factorization of n). If $\mu(\cdot)$ denotes the Möbius function, then the requirement that m is square-free and relatively prime to 210 is equivalent to $\mu^2(210m) = 1$. Fix m. Since $lk^2m^3 \leqslant x$, there are at most $\frac{\sqrt{x}}{\sqrt{m^3}}$ possible values of k and at most $1 + \log_\nu(x)$ possible values for the exponent of the prime $\nu \in \{2, 3, 5, 7\}$ in the factorization of l. Therefore, there are at most

$$\frac{\sqrt{x}}{\sqrt{m^3}} \prod_{\nu \in \{2,3,5,7\}} (1 + \log_\nu(x)) \leqslant \frac{\sqrt{x}}{\sqrt{m^3}} (1 + \log_2(x))^4 \leqslant 5 \frac{\sqrt{x}}{\sqrt{m^3}} \ln^4(2x)$$

possible choices for the pair (l,k). Hence,

$$\begin{aligned}\#A(x) &\leqslant 5\sum_{m=1}^{\infty}\mu^2(210m)\frac{\sqrt{x}}{\sqrt{m^3}}\ \ln^4(2x) \leqslant 5\sum_{m=1}^{\infty}\sqrt{210^3}\mu^2(210m)\frac{\sqrt{x}}{\sqrt{210^3m^3}}\ln^4(2x)\\ &\leqslant 5\sum_{i=1}^{\infty}\sqrt{210^3}\frac{\mu^2(i)}{\sqrt{i^3}}\ln^4(2x)\sqrt{x} \leqslant C_2\ln^4(2x)\sqrt{x},\end{aligned}$$

with $C_2 = 5\sqrt{210^3}\,\zeta(\frac{3}{2})$, where $\zeta(\cdot)$ denotes the Riemann zeta function. It follows that $\#B(x) \geqslant x - C_2\ \ln^4(2x)\ \sqrt{x}$. Now the set of primes $\leqslant x$ satisfying the hypotheses of Theorem 1.2 equals $C(x)\cap D(x)$. Therefore, the number of such primes is

$$\begin{aligned}\#C(x)+\#D(x)-\#(C(x)\cup D(x)) &\geqslant \#C(x)+\#B(x-1)-\#\{1,\cdots,x\}\\ &\geqslant C_1\frac{x}{\ln(x)}+x-1-C_2\ln^4(2x-2)\sqrt{x-1}-x\\ &= C_1\frac{x}{\ln(x)}-C_2\ln^4(2x-2)\sqrt{x-1}-1,\end{aligned}$$

which becomes unbounded as $x\to\infty$. This completes the proof. ■

References

[1] G. Andrews, R. Askey and R. Roy, *Special functions*, Encyclopedia of Mathematics and its Applications **71**, Cambridge University Press, Cambridge, 1999.

[2] F. Beukers, *On a sequence of polynomials*, J. Pure Appl. Algebra **117/118** (1997), 97–103.

[3] L. Carlitz and J. Hunter, *Sums of Powers of Fibonacci and Lucas Numbers*, Fibonacci Quart. **7** (1969), 467–473.

[4] A. Cauchy and J. Liouville, *Rapport sur un Mémoire de M. Lamé, relatif au dernier théorème de Fermat*, C. R. Acad. Sci. Paris **9** (1839), 359–363.

[5] S. Golomb, *Powerful numbers*, Amer. Math. Monthly **77** (1970), 848–855.

[6] 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.

[7] C. Helou, *Cauchy-Mirimanoff polynomials*, C. R. Math. Rep. Acad. Sci. Canada **19** (1997), 51–57.

[8] B. Irick, *Cauchy-Mirimanoff polynomials*, Ph.D. Thesis, University of Tennessee, Knoxville, 2010.

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

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

[11] M. Mignotte, T. Shorey and R. Tijdeman, *The distance between terms of an algebraic recurrence sequence*, J. Reine Angew. Math. **349** (1984), 63–76.

[12] D. Mirimanoff, *Sur l'équation* $(x+1)^l - x^l - 1 = 0$, Nouv. Ann. Math. **3** (1903), 385–397.
[13] I. Mostafa, *A new approach to polynomial identities*, Ramanujan J. **8** (2004), 423–457.
[14] J. Mott, *Eisenstein-type irreducibility criteria*, Lecture Notes in Pure and Appl. Math. 171 (1995), Dekker, New York, 307–329.
[15] T. Muir, *Cauchy's theorem regarding the divisibility of* $(x+y)^n + (-x)^n + (-y)^n$, Messenger of Math. **8(2)** (1878), 119–120.
[16] P. Nanninga, *Euclidean and Hyperbolic Diophantine Equations*, Ph.D. Thesis (submitted), Australian National University, Canberra, Australia, 2009.
[17] J.-L. Nicolas and G. Terjanian, *Une majoration de la longuer des polynômes cyclotomiques*, Enseign. Math. **(2) 45** (1999), 301–309.
[18] M. Petkŏvsek, H. Wilf and D. Zeilberger, $A = B$., A. K. Peters, Ltd. Wellesley, MA, 1996.
[19] P. Ribenboim, *Fermat's last theorem for amateurs*, Springer-Verlag, New York 1999.
[20] K. Samaké, *Suites récurrentes linéaires, problème d'effectivité*, Thèse, Université de Strasbourg I (Louis Pasteur), Strasbourg, 1996.
[21] G. Terjanian, *Sur la loi de réciprocité des puissances l-èmes*, Acta Arith. **54** (1989), 87–125.
[22] I. Todhunter, *Theory of Equations*, Macmillan and Co., London, 1861.
[23] P. Tzermias, *On Cauchy-Liouville-Mirimanoff polynomials*, Canad. Math. Bull. **50** (2007), 313–320.
[24] P. Tzermias, *Low-degree points on Hurwitz-Klein curves*, Trans. Amer. Math. Soc. **356** (2004), 939–951.
[25] P. Tzermias, *Parametrization of low-degree points on a Fermat curve*, Acta Arith. **108** (2003), 25–35.
[26] P. Tzermias, *Algebraic points of low degree on the Fermat curve of degree seven*, Manuscripta Math. **97** (1998), 483–488.
[27] J. Wimp, *Irreducible recurrences and representation theorems for* ${}_3F_2(1)$, Comput. Math. Appl. **9** (1983), 669-678.
[28] R. Wituła and D. Słota, *Cauchy, Ferrers-Jackson and Chebyshev polynomials and identities for the powers of elements of some conjugate recurrence sequences*, Cent. Eur. J. Math. **4** (2006), 531–546.
[29] D. Zeilberger, *Gauss's* ${}_2F_1(1)$ *cannot be generalized to* ${}_2F_1(x)$, J. Comput. Appl. Math. **39** (1992), 379–382.

Address: Pavlos Tzermias: Department of Mathematics, University of Patras, Rion (Patras) 26500, Greece.

E-mail: tzermias@math.upatras.gr

Received: 14 August 2010; **revised:** 2 September 2010